	A	B	C	D	E	F	G	H
1	**Id**	**Title**	**Test Step #**	**Test Step Description**	**Test Step Expected Result**	**Test Case Pass/ fail**	**Tester Name /Signature**	**Approval signature**
2	197765	Options_e-signature_editing	1	Precondition Admin User with PC time zone (Ex.PST) and OTZ (Ex. EST)				
3			2	Login as Admin user mentioned in the Precondition.	Admin user will be able to login successfully.			
4			3	Click on User Profile, click on Administrative View, click on Site Configuration, click on e-Signature Requirements, click on Edit Requirements, modify any e-signature requirement and click Save Changes.	e-Signature Required popup window will be displayed.			
5			4	Enter user id in the User ID text box. Enter password in the Password text box. Verify that Password is displayed in non-readable form for e-signature. Select a reason from the Reason for Signature drop down.	On entering Password for e-signature, password will be displayed in non-readable form			
6			5	Click on Electronically Sign.	Electronic signature will be comprised of the signer information (First Name, Last Name, User ID), date and time stamp will display based on the Admin User's PC time zone, and the meaning/reason associated with signature.			
7			6	E-signature requirements screen is displayed after e-signing the change.	Time will be displayed in PC Timezone - UTC – 8, Date will be displayed in PC Timezone - UTC – 8 and Timezone will be displayed in PC Timezone - UTC – 8.			
8			7	Try to edit the Signature field; Verify User is not able to edit Signature field.	User will not be able to edit Signature field.			
9			8	Try to delete the Signature field; Verify to see if the E-signature can be deleted.	User will not be able to delete E-signature.			
10			9	Click on Reports menu, Click Event Log Report, Click on Edit button; Remove the Existing Filter and apply filter for Admin User and event "E-signature Applied" event and click on Set as My Default button.	Event Log report with the "e-signature applied" event and Event Occurred On will be displayed with date/ time stamp based on Report time zone. Time will be displayed in Report time zone - UTC – 5, Date will be displayed in Report time zone - UTC – 5 and Timezone will be displayed in Report time zone- UTC – 5			
11			10	Click on Print button; Verify the data will display same as UI of the Event Log report and offset for Date/Time field is translated based on the Report time zone (UTC -5.00) in the printed Event Log Report.	Data in the Print Report will display same as UI of the Event Log report and offset for Event Occurred On field will be translated based on the Report time zone (UTC-5.00) in the printed Event Log Report.			
12			11	Close the Print Report Click on Download, click Excel/CSV/PDF, Verify offset for Date/Time field is translated based on the Report time zone (UTC -5.00) in the downloaded Event Log Report.	Event Log report will be downloaded in selected File type and offset for Event Occurred On field will be translated based on the Report time zone (UTC -5.00) in the downloaded Event Log Report.			
13	197766	Support_CV upload_upload & approval of CV	1	Precondition: 1. New user with pending CV with org admin rights. 2. Company CV upload file is enabled. 3. PDF file <10mb to upload				
14			2	Login as the user mentioned in the setup and click on user profile. Click on 'Curriculum Vitae' and click Upload CV	Upload CV pop-up will be displayed			
15			3	Browse the pdf file mentioned in the precondition and click on 'Upload File'	File will be uploaded to CV			
16			4	Click on 'Approve this CV' Enter valid Username and password credential of logged in user and click on Electronically sign button.	CV will be approved by the user and status of the CV changes to Effective.			
17			5	Click on User Profile, click on Administrative View, click on 'Search for Users' and search for the user mentioned in precondition.	General Information screen of the user will be displayed.			
18			6	Click on 'Curriculum Vitae' link. Click on the 'Download Curriculum Vitae' link and Verify that user is able to download the uploaded PDF	User will be able to download the uploaded pdf.			
19	197768	Users_History_Group membership history	1	**Preconditions:** 1. Admin User. 2. User Group#1 with at least 1 user added to the group by each of the below: a) Users added directly to Manually Added Users b) Users added via criteria c) Users added to Excluded User list to Manually Excluded Users				

	A	B	C	D	E	F	G	H
1	**Id**	**Title**	**Test Step #**	**Test Step Description**	**Test Step Expected Result**	**Test Case Pass/ fail**	**Tester Name /Signature**	**Approval signature**
20			2	Login as Admin User mentioned in the Precondition section; Click on User Profile, click on Administrative View and Click Administrations. Click View User Groups	User Groups page will be displayed.			
21			3	Click on the User Group#1 mentioned in Precondition section.	User Group#1 General Information page will be displayed.			
22			4	Click on Group Membership - Manually Added Users; Click on the trash icon displayed next to the user in Manually Added Users to User Group#1 and remove the User from this list.	The User in the Manually Added Users of User Group#1 will be removed from the list.			
23			5	Click on Group Membership - Manually Excluded Users; Click on the trash icon displayed next to the User in Manually Excluded Users to User Group#1 and remove the user from the list.	The User in the Manually Excluded Users of User Group#1 will be removed from the list.			
24			6	Click on 'Edit Group Criteria' from Membership Criteria and remove the saved criteria such that the User added via criteria get removed from the group. Click on 'Save Changes'.	The saved criteria through which the user added via criteria is removed from the group. The User added via criteria will be removed from the group.			
25			7	Click on 'Membership History' and verify the 'User Id', 'Last Name', 'First Name', 'Action', 'Modified By' and 'Modified On' details of the below actions are displayed correctly User Added - Manually Added User Added - Meets Criteria Membership Unchanged - Manually Excluded User Removed - Removed from Inclusion List Membership Unchanged - Removed from Exclusion List User Removed - No Longer Meets Criteria	'User Id', 'Last Name', 'First Name', 'Action', 'Modified By' and 'Modified On' details of the below actions will be displayed correctly User Added - Manually Added User Added - Meets Criteria Membership Unchanged - Manually Excluded User Removed - Removed from Inclusion List Membership Unchanged - Removed from Exclusion List User Removed - No Longer Meets Criteria			
26			8	Click anywhere on the Membership History screen and try to modify the data	Admin user will not be able to modify the data on the Group Membership History screen			
27	197770	Dashboards_Compliance Dashboard - All User Groups	1	**PRECONDITIONS:** 1. Admin user. 2. Users with different compliance status added to the Usergroup.				
28			2	Login as admin user mentioned in pre-condition, Click on User Profile, click on Administrative View, search for the user group mentioned in the precondition.	User will be able to login successfully and will navigate to user group general information page.			
29			3	Click on Membership Detail in Group Hierarchy and Verify that user is added and displays as member to the user group.	User will be added and display as member to the user group.			
30			4	Click on Dashboards tab; click on "All User Groups Dashboard" under Original Compliance Dashboards and search for the Usergroup mentioned in the precondition	Admin User will be able to search the User Group in the Compliance Dashboard - All User Groups			
31			5	Verify the Count and Percentage is displayed correctly under the respective Compliance status in the Compliance Dashboard - All User Groups screen	Count and Percentage will be displayed correctly under the respective Compliance status in the Compliance Dashboard - All User Groups screen			
32			6	Drill down on to the User Group and Verify the Count and Percentage is displayed correctly under the respective Compliance status in the Compliance Dashboard - All User Groups for the selected User Group screen	Count and Percentage will be displayed correctly under the respective Compliance status in the Compliance Dashboard - All User Groups screen for the selected User Group screen			
33			7	Click on the Count link under the respective Compliance status and verify that User details are displayed correctly as per user's compliance status.	User details will be displayed correctly as per user's compliance status.			

	A	B	C	D	E	F	G	H
1	**Id**	**Title**	**Test Step #**	**Test Step Description**	**Test Step Expected Result**	**Test Case Pass/ fail**	**Tester Name /Signature**	**Approval signature**
34	197772	Users_Forget User	1	Precondition: Company with 'Allow to Forget User' preference enabled. Test user#1Admin user				
35			2	Login as admin user mentioned in the setup, Click on User Profile, click on Administrative View; Search for the Test User#1 mentioned in precondition; Click on 'Forget User' link.	User will be navigated to Forget User page			
36			3	Enter a new user Id which is unique in the New Replacement User Id text box and click on 'Continue' button; Enter valid e-signature details, select Reason for Signature and enter Signature Comment. Click on 'Electronically Sign'.	A "Your Forget User request has been submitted for processing. The status of this request can be seen from the user's General Information view." will be displayed.			
37			4	Click on the 'Return' button in confirmation page	Admin user will be navigated to the User's General Information screen of the user for the forget user request has been initiated.			
38			5	Verify the user's General Information displays replacement user id provided as the New User id and the Status of the Forget User Request as either Pending or In-Progress or completed based on system queue length.	The user's General Information will display replacement user id provided as the New User id and the Status of the Forget User Request as either Pending or In-Progress or completed based on system queue length.			
39			6	Verify the user's First Name, Middle Name, Last Name, and all the personal information are obfuscated when the Forget User Request updates to Completed. Verify user is disabled.	User's First Name, Middle Name, Last Name, and all the personal information will be obfuscated when the Forget User Request updates to Completed. User will get disabled.			
40			7	Verify the Signature field under "Forget User Request Information" section is non editable.	The Signature field under "Forget User Request Information" section will not be editable.			
41			8	Click on Reports and click on 'Event Log Report' link.	Admin User will be navigated to the Event Log Report page.			
42			9	Generate an event log report for the admin user for the below selected events: Forget User request initiated Forget User request completede-Signature Applied	Data in the selected the fields will be displayed correctly in the generated Event Log report for the below events: Forget User request initiated Forget User request completede-Signature Applied			
43			10	Click on any row for below events and verify Admin User is navigated to the User General Information screen.	Admin User will be navigated to the User General Information screen.			
44	195623	Knowledge center_e-sign_date and timestamp	1	Precondition: 1. Instructor Led Course with a Class, both with online registration ON 2. Require e-signatures for Student Online Registration ENABLED 3. Learner				
45			2	Login as Learner noted in Precondition section.	Learner will be able to login successfully.			
46			3	Click Catalog.Search for the training noted in Setup and click to view course information	Learner will be able to navigated to Catalog page and view the course information.			
47			4	Click on class information link and click on class code to register, Click register for a class.	e-Signature Required popup window will be displayed.			
48			5	Enter User ID and Password.Verify that Password is displayed in non-readable form for e-signature	On entering Password for e-signature, password will be displayed in non-readable form			
49			6	Click Electronically Sign.Search for the training noted in Setup in the To- Do list and click to view course information.Click on Class information link.	Learner will be able to self-register for the ILC class requiring an e-signature. The ILC information window will display the class information with the e-signature having date and time stamp based on User's PC time zone.			
50			7	Click on Drop Class. Enter the eSignature details in the e-Signature popup and electronically signin	Training item should be dropped and will no longer appear in the ToDo list.			
51	195637	Knowledge Center_CustomExam_e-sign	1	Precondition: 1. Custom Exam 2. e-signatures enabled for custom exam completions 3. Learner				
52			2	Login as Learner noted in Precondition section.	Learner will be able to login successfully.			

	A	B	C	D	E	F	G	H
1	**Id**	**Title**	**Test Step #**	**Test Step Description**	**Test Step Expected Result**	**Test Case Pass/ fail**	**Tester Name /Signature**	**Approval signature**
53			3	Click Catalog	Learner will be able to navigated to Catalog page.			
54			4	Search and complete the training in Setup, electronically signing for completion	e-Signature window will be displayed.			
55			5	Verify that Password is displayed in non-readable form for e-signature	On entering Password for e-signature, password will be displayed in non-readable form			
56			6	Click History	Learner will be able to navigated to History page.			
57			7	Click on the TI completed and View the completion information for the training.	Completion information screen will display the User, Training and the completion Information. Completion date will be displayed based on the Learner's OTZ and e-signature field will display date and time stamp based on User's PC time zone.			
58	195643	Users_User Histroy_View User History	1	Precondition 1. Admin User				
59			2	Login as Admin user. Click on User Profile, click on Administrative View	Admin Home should be displayed.			
60			3	Click Add User	Add user page should be displayed			
61			4	Enter valid data in the required fields and click Save	Required fields data should be saved and displayed in General Information screen.			
62			5	Click General Information and click on History link.	The initial creation information will include date, time and who created (Created by and Created On) in User Account History screen.			
63			6	Click Edit User, edit any field(s), click Save Changes	General Information screen is displayed with the changes made.			
64			7	Click History link.	User Account History will display the property edited, old value, new value, user making the change and the date/time of the change.			
65			8	Click on General Information and Repeat steps 5 - 6 and verify the changes in the History.	User Account History will display an entry for each property change.			
66			9	Click anywhere on the history screen, on any record, in an attempt to change any data displayed	The user will not be able to change any of the historical data recorded for this user.			
67	195644	Users_Add User_Existing UserID	1	Precondition 1. Admin User				
68			2	Login as admin user as mentioned in precondition	Admin user will be able to login successfully.			
69			3	Click on User Profile, click on Administrative View and Click Add User.	Add user screen should be displayed			
70			4	Enter valid data in the First Name, Last Name text box. Enter the User Id same as that is mentioned in the setup in the User ID text box. Enter valid data in the Password and Confirm Password text boxes. Click Save.	User is able to enter the values in First Name, Last Name and User ID textboxes. A Pop up with a message "The User Id you entered already exists in this Company" will display indicating User ID entered already exists in the company and the new user will not be created			
71	195645	Users_SecurityRole_Overriding SecurityRole	1	Precondition 1. Test user with full rights (not an org admin) in any middle org and a learner security role in a lower org. 2. Training homed in and below the level of the role with full rights. 3.Training homed in and below the level of role with learner				

	A	B	C	D	E	F	G	H
1	**Id**	**Title**	**Test Step #**	**Test Step Description**	**Test Step Expected Result**	**Test Case Pass/ fail**	**Tester Name /Signature**	**Approval signature**
72			2	Login as test user as mentioned in precondition 1	Test user will be able to login successfully			
73			3	Click on User Profile, click on Administrative View	Admin Home should be displayed.			
74			4	View and edit trainings assigned in the same org as the role with full rights.	User will be able to view and edit training assigned in the same org containing the role with full rights.			
75			5	View and edit training assigned in orgs at lower levels	User will not be able to view and edit training assigned in the same org as the org containing the Learner role and orgs below that level.			
76	195646	Users_SecurityRole_Grant SecurityRole	1	Precondition 1. Admin User 2. Test User w/ security role containing rights: 'View users', 'Define, edit, or remove security roles' right.				
77			2	Login as Test user as mentioned in precondition	Test user will able to login successfully.			
78			3	Click on User Profile, click on Administrative View and click 'Site Configuration'. Click on 'Security Roles' under Security and Access Controls	Security Roles page should be displayed			
79			4	Click on 'Add New Security Role' .Select an organization for the role and click 'Continue'. Verify user does not have access to select rights which the user's security role does not have.	User will not have access to select rights which the user's security role does not have.			
80			5	Verify user is able to select same or lesser rights granted to them in their own security role. Select few security rights and click on 'Add'.	User will be able to select same or lesser rights granted to them in their own security role. New Security role with select security rights will be created.			
81			6	Sign out and login as the Admin user mentioned in setup. Click on User Profile, click on Administrative View, click 'Reports' and click on 'Event Log Report'. Click on Edit button; Apply Filter for user id of the test user and Select the event as "Add security role" and click on 'Run Report Without Saving.	The event log report will be generated and will display Add security role event record.			
82			7	Sign out and login as the test user mentioned in setup. Click on User Profile, click on Administrative View, and click 'Site Configuration'. Click on 'Security Roles' and click on a security role	The Security Role details page will be displayed.			
83			8	Click Edit Security Role created above, make some changes and click 'Save'.	Verify that the user is able to edit the security role by adding or removing a security bit that the user has same rights defined with.			
84			9	Sign out and login as the Admin user mentioned in setup. Click on User Profile, click on Administrative View, click 'Reports' and click on 'Event Log Report'. Click on Edit button; Apply Filter for user id of the test user and Select the event as "Edit security role" and click on 'Run Report Without Saving	The event log report will be generated and will display Edit security role event record.			
85			10	Sign out and login as the test user mentioned in setup. Click on User Profile, click on Administrative View, and click 'Site Configuration'. Click on 'Security Roles' and click on a security role.	The Security Role details page will be displayed.			
86			11	Click on 'Remove Security Role'. Click 'OK' in the Pop up screen.	The selected Security role will be removed.			
87			12	Sign out and login as the Admin user mentioned in setup. Click on User Profile, click on Administrative View, click 'Reports' and click on 'Event Log Report'. Click on Edit button; Apply Filter for user id of the test user and Select the event as "Remove security role" and click on 'Run Report Without Saving	The event log report will be generated and will display Remove security role event record.			
88			13	Click Edit, Click Settings and select Report Time Zone other than the user OTZ and run the report	Date/TIme in the Event Occurred On column will be updated based on the report time zone selected in Settings			
89	195647	Users_Security Role_Assign & Override security role	1	Precondition 1. Admin User. 2. Security role 3. Two users whose User Id and/or Last Name and/or First Name containing common characters 4. One with a role assigned in a specific organization and one w/o a role in the mentioned organization.				
90			2	Login as Admin User mentioned in the Precondition	Admin user will be able to login successfully			

	A	B	C	D	E	F	G	H
1	**Id**	**Title**	**Test Step #**	**Test Step Description**	**Test Step Expected Result**	**Test Case Pass/ fail**	**Tester Name /Signature**	**Approval signature**
91			3	Click on User Profile, click on Administrative View and click 'Site Configuration'. Click on 'Security Roles' under Security and Access Controls. Click on the security role mentioned in Precondition section.	Security role should be selected			
92			4	Click Assign Security Role. Select the organization mentioned in Precondition section and click Continue	The Assign Security Role to Users pop up window will display the organization.			
93			5	Search for the users mentioned in setup	The "Assign Security Role" link will be displayed only after user does user search.			
94			6	Verify that by default the users w/o a role in the organization are selected and the users with a role in the organization are not selectable	Security role can be assigned to all the users who do not have a role in the selected organization.			
95			7	Click Assign Security Role. Click Users link displayed in the left console and Click on "Assign Security Role" button.	Security Role cannot be assigned to users who have a role in the selected organization.			
96			8	Click Reports, Click Event Log Report.	The Event Log Report screen will be displayed.			
97			9	Click on Edit, click on Filters, remove existing saved filters, select "Event" as filter type, select "is" as operator, search and select "Add security role to user" event from the value dropdown and click on "Run Report without Saving" button.	The Event log will display the "Add security Role to user" record with the date/timestamp based on report time zone.			
98			10	Click on the row for the event "Add Security Role to the User" and verify Admin User is navigated to the User General Information screen.	Admin User is navigated to the User General Information screen			
99			11	Click 'Site Configuration'. Click on 'Security Roles' under Security and Access Controls ,click on the security role mentioned in the precondition; Click on Assign Security Role link; Select the organization in which the tester has "Org. Administrator" role.	The Assign Security Role to Users pop up window will display the organization.			
100			12	Search for the users mentioned in setup. Check the checkbox "Allow override of existing Security Roles"	User will be able to use checkbox			
101			13	Select the user w/security role mentioned in setup from the search result list. Click Assign Security Role. Click Users link displayed in the left console	Security roles of the users in the organization will be over-ridded by the selected security role using user search option.			
102	195649	Users_Security roles_assigning security role	1	Precondition: 1. User with org admin rights 2. Security Role				
103			2	Login as the Admin User as mentioned in precondition	Admin user will be able to login successfully			
104			3	Click on User Profile, click on Administrative View and click 'Site Configuration'. Click on 'Security Roles' under Security and Access Controls. Click on the Security role mentioned in Precondition section.	Security role will be selected			
105			4	Click Assign Security Role. Select the organization in which the tester has "Org. Administrator" role.	Admin user will be able to access assign security role page			
106			5	Search for own user id. Check the checkbox "Allow override of existing Security Roles". Try to Select own user id.	System will not allow the user to change their own security role while trying to assign a security role to multiple users.			

	A	B	C	D	E	F	G	H
1	**Id**	**Title**	**Test Step #**	**Test Step Description**	**Test Step Expected Result**	**Test Case Pass/ fail**	**Tester Name /Signature**	**Approval signature**
107	195650	Users_Group memberships_Manage group memberships	1	Precondition: 1. Testuser w/'View Users', 'View User Groups', 'Manage Group Membership' rights in any middle level organization 2. User Groups homed above, at and below the organization in which the user's role assigned.				
108			2	Login as Test user. Click on User Profile, click on Administrative View, Search for the User Group homed in the same organization where user's role assigned	General Information screen of the user group will be displayed.			
109			3	Edit Group membership by adding, removing and excluding users homed in directly from User Group.	User will be able to Manage Group memberships for User groups homed at the organization in which their role is assigned.			
110			4	Repeat the previous steps for the User Groups homed above and below the organization where user's role is assigned.	User will be able to Manage Group memberships for User groups homed below the organization in which their role is assigned. User will NOT be able to Manage Group memberships for User groups homed above the organization in which their role is assigned as the user cannot access the group.			
111	195651	User_Credit History	1	Precondition: 1. EDUADMIN preference Credit - Grant for the company is turned ON. 2. EDUADMIN preference Credit - Request/Approval for the company is turned ON. 3. Admin User with PC Time Zone set. 4. Preferred Time Format set as "h:mm:ss tt UTC ±xx" for the above Admin User.5. User 6. Admin User is a manager for user 7. Credits rejected for the Training Item #1 being requested by the above User. 8. Credits approved for the Training Item#1 being requested by the above User. 9. Credit granted for the above Training Item#2 being assigned to the above User. 10. Credit removed for the Training Item#2 being granted to the above User				
112			2	Login as Admin User mentioned in the setup.	Admin User will be able to login successfully			
113			3	Click on User Profile, click on Administrative View, Search for the User mentioned in the setup.	Admin User will be navigated to the searched User General Information screen.			
114			4	Click on View Credit History link and verify the Admin User is able to view ComplianceWire Header & footer.	Admin User will be able to view ComplianceWire Header & footer.			
115			5	Verify that Admin User is able to view Page Name.	Admin User will be able to view Page Name.			
116			6	Verify that User Information section is displayed appropriately in the following order: • User ID. • Last Name. • First Name.	User Information section will be displayed appropriately in the following order: • User ID. • Last Name. • First Name.			
117			7	Verify the following columns are displayed appropriately to the Admin User in the Credit History screen of the User • Training Title for the training item for which credit is received. • Training Code for the training item for which credit is received. • Training Version for the training item for which credit is received. • Training Type for the training item for which credit is received. • Action. • Modified By. • Modified On.	Following columns are displayed appropriately to the Admin User in the Credit History screen of the User • Training Title for the training item for which credit is received. • Training Code for the training item for which credit is received. • Training Version for the training item for which credit is received. • Training Type for the training item for which credit is received. • Action. • Modified By. • Modified On.			
118			8	Verify the Modified By column displayed as Last Name, First Name (user id) of the person who is performing the action.	Modified By column will be displayed as Last Name, First Name (user id) of the person who is performing the action.			

	A	B	C	D	E	F	G	H
1	**Id**	**Title**	**Test Step #**	**Test Step Description**	**Test Step Expected Result**	**Test Case Pass/ fail**	**Tester Name /Signature**	**Approval signature**
119			9	Verify the date and offset value for Modified On field is displayed (when the Action is performed) and translated based on the Admin User PC Time Zone.	Date and offset value for Modified On field will be displayed (when the Action is performed) and translated based on the Admin User PC Time Zone			
120			10	Try to edit any section/fields/records in the Credit History screen. Verify that Admin User will not be able to edit the Credit History screen.	Admin User will not be able to edit the Credit History screen.			
121			11	Click Reports; Click on Event Log Report; Generate the Event log report for the below Events: 1. Credit Removed. 2. Credit Approved. 3. Credit Rejected. 4. Credit Granted.	Data in the selected the fields will be displayed correctly in the generated Event Log report for the below events: 1. Credit Removed. 2. Credit Approved. 3. Credit Rejected. 4. Credit Granted.			
122	195652	Users_Organization and Role History	1	Precondition: 1. Admin User 2. User with different security roles in different Organizations.				
123			2	Login as admin user mentioned in the precondition, Click on User Profile, click on Administrative View and search for User.	General Information of User will be displayed.			
124			3	Click on 'Organization and Role History'. Verify the following details are displayed correctly in the Organization and Role History screen: * First Name * Last Name * User Id * Created On * Created by	Following details displayed correctly in the Organization and Role History screen: * First Name * Last Name * User Id * Created On * Created by			
125			4	Verify the below columns with correct data are displayed in the Organization and Role History screen: * Organization Name/Entity * Security Role * Custom Attribute Value Filter * Action * Last Modified By * Last Modified Date	Columns with correct data are displayed in the Organization and Role History screen: * Organization Name/Entity * Security Role * Custom Attribute Value Filter * Action * Last Modified By * Last Modified Date			
126			5	Try to edit any section/fields/records in the Users Organization and Role History screen. Verify that Admin User will not be able to edit the Organization and Role History screen.	Admin User will not be able to edit the Organization and Role History screen.			
127	195653	User Group_Group Criteria Change Log page	1	**Precondition**: 1. Admin user with a set OTZ (example PST). 2. User Group #1(regular group) that have a some criteria set for group membership. 3. User Group #2(meta group) that have a some criteria set for group membership. 4. User Group #3 that has no criteria set for group membership. 5. Admin user's Preferred Date (display format setting) and time set to mm/dd/yyyy and "h:mm:ss tt UTC±xx". 6. Admin user's PC time zone set to a time zone other than the set OTZ (example EST).				
128			2	Login as the admin user specified in the setup. Click on User Profile, click on Administrative View	Admin user will be able to navigate to Admin Home tab.			
129			3	Search for the User Group #1 mentioned in the Precondition.	Admin user will be navigated to the Group Information page.			
130			4	Click on the link "Criteria Change Log" and verify the user is navigated to the " Criteria Change Log" page.	Admin user will be navigated to " Criteria Change Log" page.			
131			5	Verify that the page displays ComplianceWire Header, footer with UL logo, links to view the copyright, Terms of Use and System Information	The page will display ComplianceWire Header, UL logo, links to view the copyright, Terms of Use and System Information.			

	A	B	C	D	E	F	G	H
1	**Id**	**Title**	**Test Step #**	**Test Step Description**	**Test Step Expected Result**	**Test Case Pass/ fail**	**Tester Name /Signature**	**Approval signature**
132			6	Click on all the links in the footer and ensure that each link opens the respective window.	All the links in the footer will be clickable and each link will open a respective window.			
133			7	Verify that the following columns appear in the below order: 1. Criteria 2. Action 3. Modified By 4. Modified On	The following columns will appear in the below order: 1. Criteria 2. Action 3. Modified By 4. Modified On			
134			8	Verify that the Modified On as Date & Time is displayed in user's preferred date/time format.	The Modified On as Date & Time will be displayed in user's preferred date/time format.			
135			9	Verify that the Modified On will display the offset as part of date/time.	The Modified On will display the offset as part of date/time.			
136			10	Verify the Modified On is displayed as admin user's PC time zone and not admin user's OTZ.	The Modified On will be displayed as admin user's PC time zone and not admin user's OTZ.			
137			11	Verify that the Criteria Change Log page has links for print and download.	The Criteria Change Log page will have links for print and download.			
138			12	Try to edit any section in the Criteria Change Log screen	Admin User will not be able to edit any section in the generated Criteria Change Log screen.			
139			13	Search for the User Group #2 mentioned in the Precondition and click Criteria Change Log	User will be navigated to " Criteria Change Log" page. The UI of " Criteria Change Log" page of the metagroup will be the same as that of the regular group. All the links in the footer will be clickable and each link will open a respective window.			
140			14	Try to edit any section in the Criteria Change Log screen	Admin User will not be able to edit any section in the generated Criteria Change Log screen.			
141			15	Search for the User Group #3 mentioned in the Precondition and click Criteria Change Log	Clicking " Criteria Change Log" link user will be navigated to "Criteria Change Log" page.			
142			16	Verify that no data is displayed under the below columns: 1. Criteria 2. Action 3. Modified By 4. Modified On	No data will be displayed under the below columns: 1. Criteria 2. Action 3. Modified By 4. Modified On			
143			17	Try to edit any section in the Criteria Change Log screen	Admin User will not be able to edit any section in the generated Criteria Change Log screen.			
144	195654	Users_User_Disable_Enable User	1	Precondition: 1. Admin User 2. Enabled User				
145			2	Login as admin user mentioned in the precondition, Click on User Profile, click on Administrative View, search for user mentioned in precondition.	Admin User will be able to login successfully and will navigated to user general information page.			
146			3	Click 'Disable User Account' link displayed in left navigation of the user.	User will navigate to Disable a User window			

	A	B	C	D	E	F	G	H
1	**Id**	**Title**	**Test Step #**	**Test Step Description**	**Test Step Expected Result**	**Test Case Pass/ fail**	**Tester Name /Signature**	**Approval signature**
147			4	Verify "Disabling a User will remove their incomplete assignments" warning message is displayed.	A "Disabling a User will remove their incomplete assignments" warning message will be displayed.			
148			5	Click on 'Disable This User'.	User will be disabled and admin user will navigate to general information page of disabled user.			
149			6	Verify that User's Current Status is displayed as Disabled.	User's Current Status will be displayed as Disabled.			
150			7	Click on "Enable User Account" link; Verify that User's Current Status is updated to Enabled.	User's Current Status will be displayed as Enabled.			
151			8	Click Reports; Generate Event log report for the below events and Verify the data in all the fields are displayed correctly in the generated Event Log report. 1. Enable User. 2. Disable User	Data in the selected the fields will be displayed correctly in the generated Event Log report for the below events: 1. Enable User. 2. Disable User			
152			9	Try to edit the above generated event log report. Verify that Admin User will not be able to edit the generated event log report.	Admin User will not be able to edit the generated event log report.			
153			10	Click on any row for the below events and verify Admin User is navigated to the User General Information screen. 1. Enable User. 2. Disable User	Admin User will be navigated to the User General Information screen by clicking row related to disable user. Admin User will be navigated to the User General Information screen by clicking row related to enable user.			
154			11	Disable the above User; Verify that Admin User will be able to disable the enabled User.	Admin User will be able to disable the enabled User.			
155			12	Sign out and Try to login as the above disabled User.	The message "The combination of User ID, Password, and Company Code entered are incorrect or the account you have entered is disabled or does not exist. Please try again or contact your system administrator." will be displayed upon login with the disabled User.			
156	195658	Training_Class roster_view	1	Precondition: 1.Instructor Led Course with class with Self registration enabled 2. User self registered for the class. 3. User with roster completion for above ILC TI. 4. Admin user				
157			2	Login as Admin. Click on User Profile, click on Administrative View; Search for the training noted in Precondition section.	User will be navigated to Training General information screen.			
158			3	Click Classes, Click on Class noted in precondition, Click on Roster History	The Class Roster History will be displayed an entry for the user who registered online and will show a status of Incomplete.			
159			4	Verify the recent completion recorded for user mentioned in Precondition 3 .	Recent completion will be recorded for user			
160			5	Select Current Roster link in the left navigation panel.	The current roster screen will be displayed.			
161			6	Click on Manage completion Icon and update the completion with Completion Date and Completions (Qualified or Not Qualified) for the user.	The completion will be updated in the Current Roster Screen			

	A	B	C	D	E	F	G	H
1	**Id**	**Title**	**Test Step #**	**Test Step Description**	**Test Step Expected Result**	**Test Case Pass/ fail**	**Tester Name /Signature**	**Approval signature**
162			7	Click on View Completion Information Icon; Verify the details are displayed correctly in the Completion Information page for the selected User and ILC Training Item.	Details will be displayed correctly in the Completion Information page for the selected User and ILC Training Item.			
163			8	Click on Roster History in the left navigation panel; Note the completion records for the user with multiple completions	Roster History will be provided every recorded completion for the class.			
164	195659	Training_Training report generation rights	1	Precondition: 1. Test User#1 without rights to Manage Quick Reports. 2. Test User#2 without the rights to any training security bits. 3. Test User#3 with rights to Manage Quick Reports. 4.Training item#1				
165			2	Login as Test User#1 mentioned in Precondition#1. Click on User Profile, click on Administrative View, Search Training item#1 and Click on Quick Reports.	Reports in Quick Report page should be displayed only with Run option.			
166			3	Run any quick report and ensure edit option is not displayed in the report	Quick report should be displayed with Print and Download options and without the edit option.			
167			4	Sign out and login as Test User#2 mentioned in Precondition#2. Click on User Profile, click on Administrative View, Verify training related info is not displayed in admin home	Training related info is not displayed in Admin Home			
168			5	Sign out and login as Test User#3 mentioned in Precondition#3. Click on User Profile, click on Administrative View, Search Training item#1 and Click on Quick Reports.	Reports in Quick Report page should be displayed with Run, Edit and disable options			
169			6	Click on any quick reports and ensure edit button is displayed in the report	Quick report should be displayed with Edit, Print and Download options			
170	195660	Training_Security rights_Curriculum Quick Reports	1	Precondition: 1. Admin user 2. Test user 3. Assignments and completions for curriculum.				
171			2	Login as the Admin user. Click on User Profile, click on Administrative View and Click Site Configuration, Add a security role, with the following enabled -View training items, classes, rosters -View Curriculum-Manage Curriculum -View Completions by Training-View Assignments by Training -Manage Quick Reports for Training & Curriculum	The Security role will be created with the rights.			
172			3	Assign the new security role to a Test User	New security role is assigned to the user.			
173			4	Log on as the Test User, Click on User Profile, click on Administrative View, Search the Curriculum mentioned in the precondition. Click on Quick Reports; Click on Actions in the banner; Click on Create an Assignment Quick Report ; Click on Edit button; Click on Save as New Quick Report; Enter the Report Name and Description; Click on Save button.	The Test User will be able to generate an Assignment Quick Report By Curriculum			
174			5	Navigate back to the Quick Reports screen; Click on Actions in the banner; Click on Create an Completions Quick Report ; Click on Edit button; Click on Save as New Quick Report; Enter the Report Name and Description; Click on Save button.	The test user will be able to create a Completion Quick Report By Curriculum			
175			6	Access Curriculum General Information screen, Click Quick Reports, and Click on each quick report created	Saved quick report will be displayed			
176			7	User Will be navigated to Quick Reports page, Delete quick reports	Delete Quick Report modal will be displayed			

	A	B	C	D	E	F	G	H
1	**Id**	**Title**	**Test Step #**	**Test Step Description**	**Test Step Expected Result**	**Test Case Pass/ fail**	**Tester Name /Signature**	**Approval signature**
177	195661	Training_CD completions_E-signatures for completions	1	Precondition: 1. E-signature for CD completions is enabled. 2. Control Document. 3. Above control document assigned to a Learner user. 4. Admin User.				
178			2	Login as Learner User mentioned in the Precondition 3 and complete the CD and E-sign for the completion.	Learner user will be able to complete the CD with E-sign.			
179			3	Click on the History tab to view the completion history of the TI mentioned in the precondition	The history of the TI will display the Completion Date. The completion date will be displayed based on the Learner's OTZ and e-signature field will display date and time stamp based on User's PC TZ.			
180			4	Login as the Admin User mentioned in the Precondition 4.	The knowledge center screen is displayed.			
181			5	Click on User Profile, click on Administrative View and Click Reports. Click on Completion Report by Training. Generate the Report for the above user and training item.	Completion Report displays the Completion Date based on the Learner User's Operative time zone.			
182			6	Click on the row with Training item in the Completion Report by Training and Verify all the details are displayed correctly in the Completion General Information page.	Completion date will be displayed based on the Learner User's Operative Time zone and e-signature field will display date and time stamp based on User's PC TZ in the Completion Information page.			
183			7	Click on Remove Completion under Actions and Click on Remove Button in the Remove Completion Modal. Enter all the required details and click on Electronically Signature Button. Verify Completion is removed, user stays on Completion General Information screen, Completion Status is displayed as Removed. Verify Actions menu is greyed out and unable to view Certificate of Completion after completion removal.	Completion will be removed, user will stay on Completion General Information screen, Completion Status will be displayed as Removed. Actions menu will be greyed out and unable to view Certificate of Completion after completion removal.			
184			8	Verify below details are displayed in Removed Completion Information GI screen. REMOVED BY : Last Name, First Name (User ID) REMOVED ON : Date/Time Format: Show Offset Value PC Time Zone: UTC-XX	Below details will be displayed in Removed Completion Information GI screen. REMOVED BY : Last Name, First Name (User ID) REMOVED ON : Date/Time Format: Show Offset Value PC Time Zone: UTC-XX			
185			9	Click on Return to Report link and Verify user is navigated back to the report and the record count is decremented in the generated Completion Report upon removing learner completion.	User will be navigated back to the report and "No records found" is displayed in the generated Completion Report upon removing learner completion.			
186			10	Click on Reports menu, click on Event Log Report, apply filters for the below events and Run the Report. 1. e-Signature Applied 2. Score Added 3. Score Removed Verify Records are displayed based on the applied filter criteria in the generated Report: Verify below details are displayed correctly for events: 1. Event: e-Signature Applied, Score Added and Score Removed 2. Event Occurred ON: Date and time when the event is performed. 3. Event Created By User ID: User ID of Admin User for e-Signature Applied & Score Removed events and User ID of Learner User for Score Added event	Records will be displayed based on the applied filter criteria in the generated Report: Below details will be displayed correctly for events: 1. Event: e-Signature Applied, Score Added and Score Removed 2. Event Occurred ON: Date and time when the event is performed. 3. Event Created By User ID: User ID of Admin User for e-Signature Applied & Score Removed events and User ID of Learner User for Score Added event			
187			11	Sign out and Login as Learner, access History and Verify Completion for Learner and CD Training Item is no more displayed in the History screen.	Completion for Learner and CD Training Item will no more displayed in the History screen.			
188	195662	Training_History_TI history	1	Precondition: 1. Admin User				
189			2	Login as the admin user mentioned in the setup. Click on User Profile, click on Administrative View; Add a training item. Click on Training Item History, verify the changes have been recorded.	The training item history screen will provide a chronological history of all changes made.			
190			3	Click General Information and Click Edit General Information, make multiple modifications, click Save Changes. Click Training Item History	The property edited, old and new values, the user who made change, and date/time of change will be displayed			

	A	B	C	D	E	F	G	H
1	**Id**	**Title**	**Test Step #**	**Test Step Description**	**Test Step Expected Result**	**Test Case Pass/ fail**	**Tester Name /Signature**	**Approval signature**
191	195663	Training_Credit History	1	Precondition: 1. EDUADMIN preference Credit - Grant for the company is turned ON. 2. EDUADMIN preference Credit - Request/Approval for the company is turned ON. 3. Admin User with PC Time Zone set. 4. Preferred Time Format set as "h:mm:ss tt UTC±xx" for the above Admin User. 5. Training Item. 6. User#1 who is an Admin. 7. User#2,User#3 who is a Learner. 8. Admin User is a manager for user#1,user#2 & user#3 9. Credits rejected for the above Training Item being requested by the User#1. 10. Credits approved for the Training Item being requested by the User#1. 11. Credits requested for the Training Item being assigned to the User#2. 12. Credits closed for the Training Item being requested by the User#2. 13. Credit granted for the above Training Item being assigned to the User#3 14. Credit removed for the Training Item being granted to the User#3				
192			2	Login as Admin User mentioned in the setup.	Admin User will be able to login successfully			
193			3	Click on User Profile, click on Administrative View, Search for the Training Item mentioned in the Precondition.	Admin User will be navigated to the searched Training Item General Information screen.			
194			4	Click on Credit History link in the Left Navigation and verify the Admin User is able to view ComplianceWire Header & footer.	Admin User will be able to view ComplianceWire Header & footer			
195			5	Verify that Admin User is able to view Page Name.	Admin User will be able to view Page Name.			
196			6	Verify that TRAINING Information section is displayed appropriately in the following order:Title.Code.Version.Type	TRAINING Information section will be displayed appropriately in the following order:Title.Code.Version.Type			
197			7	Verify the following columns with data are displayed appropriately to the Admin User in the Credit History screen of the Training Item User ID. Last Name. First Name. Action. Modified By. Modified On.	Following columns with data will be displayed appropriately to the Admin User in the Credit History screen of the Training Item User ID. Last Name. First Name. Action. Modified By. Modified On.			
198			8	Verify the Modified By column displayed as Last Name, First Name (user id) of the person who is performing the action.	Modified By column will be displayed as Last Name, First Name (user id) of the person who is performing the action.			
199			9	Verify the date and offset value for Modified On field is displayed (when the Action is performed) and translated based on the Admin User PC Time Zone.	Date and offset value for Modified On field will be displayed (when the Action is performed) and translated based on the Admin User PC Time Zone			
200			10	Try to edit any section/fields/records in the Credit History screen. Verify that Admin User will not be able to edit the Credit History screen.	Admin User will not be able to edit the Credit History screen.			
201			11	Click Reports; Click on Event Log Report; Generate the Event log report for the below Events: Credit Removed.Credit Approved.Credit Rejected.Credit Granted.	Data in the selected the fields will be displayed correctly in the generated Event Log report for the below events:Credit Removed.Credit Approved.Credit Rejected.Credit Granted.			
202	195664	Training_Curriculum_Training in Curriculum History	1	Precondition: 1. Admin User with PC Time Zone set. 2. Curriculum. 3. Training Items added and removed directly to and from the above Curriculum respectively.				
203			2	Login as Admin User mentioned in the setup.	The user is logged in successfully			
204			3	Click on User Profile, click on Administrative View	Admin Home Page will be displayed.			
205			4	Search for the Curriculum mentioned in the setup.	The User is able to search for the curriculum and Curriculum general information Page is populated			
206			5	Click on Training in Curriculum History link.	Training in Curriculum History is populated			
207			6	Verify the Admin User is able to view ComplianceWire Header & footer	Admin User will be able to view Compliance Wire Header & footer in the Training In Curriculum History screen.			

	A	B	C	D	E	F	G	H
1	**Id**	**Title**	**Test Step #**	**Test Step Description**	**Test Step Expected Result**	**Test Case Pass/ fail**	**Tester Name /Signature**	**Approval signature**
208			7	Verify the below columns with data appear appropriately in the Training In Curriculum History screen. i Training ii Action iii. Modified By. iv. Modified On.	The below columns with data appear appropriately in the Training In Curriculum History screen of the Curriculum: i Training ii. Action iii. Modified By. iv. Modified On.			
209			8	Verify the Modified By column displayed as Last Name, First Name (user id).	Modified By field will be displayed as Last Name, First Name (user id).			
210			9	Verify that Modified On field is sorted in descending order by default in the Training In Curriculum History screen for a Curriculum.	Modified On field will be sorted in descending order by default in the Training In Curriculum History screen for a Curriculum.			
211			10	Verify the date and offset value for Modified On field is translated based on the Admin User PC Time Zone.	Date and offset value for Modified On field will be translated based on the Admin User PC Time Zone.			
212			11	Click on the column header of Training to sort.	The column Training is sorted			
213			12	Click on the same column header to re-sort the order	The column Training is re-sorted			
214			13	Repeat steps 12 and 13 for the following Column headers: i Action ii Modified By.	Training In Curriculum History screen list will be sorted according to the column header selected.			
215			14	Verify that the list displays with the "Up" icon when the current sort is ascending.	List will be displayed with the "Up" icon when the current sort is ascending for the selected column.			
216			15	Verify that the list displays with the "Down" icon when the current sort is descending.	List will be displayed with the "Down' icon when the current sort is descending for the selected column.			
217			16	If the list spans more than 1 page, click on the Page # and verify that Admin User is taken to corresponding page and current sort is retained on the current header.	Admin User will be navigated to corresponding page and current sort will be retained on the current header.			
218			17	Verify that Admin User is not able to change the order of the columns in the Training Item History screen.	Admin User will not be able to change the order of the columns			
219			18	Verify the record count is displayed appropriately in the Training In Curriculum History screen.	Records count will be displayed appropriately in the Training In Curriculum History screen.			
220	195667	Login_Users login_Login missing forgotten password questions	1	Precondition: 1. Reset Forgotten Password option enabled 2. Force answer question option enabled. 3. New user who has NOT provided answers to security questions for the forgotten password reminder feature 4. Admin User.				
221			2	As the user mentioned in Precondition section, access CW login screen. Verify ULTRUS logo with updated Header and Footer and ULTRUS color is applied to the below Web Elements in Login Page: 1. Welcome Text (including the background and the "Learn More" button text.) 2. I Accept button	ULTRUS logo with updated Header and Footer and ULTRUS color will be applied to the below in Login Page: 1. Welcome Text (including the background and the "Learn More" button text.) 2. I Accept button			
222			3	Enter valid user id in the User Id field. Enter invalid password in the Password field. Enter company code in the Company Code field. Click I Accept	Warning message displayed as "The combination of User ID, Password, and Company Code entered are incorrect or the account you have entered is disabled or does not exist. Please try again or contact your system administrator." and User not be able to login to CW.			

	A	B	C	D	E	F	G	H
1	**Id**	**Title**	**Test Step #**	**Test Step Description**	**Test Step Expected Result**	**Test Case Pass/ fail**	**Tester Name /Signature**	**Approval signature**
223			4	Again enter valid user id in the User Id field.Enter valid password in the Password field. Enter company code in the Company Code field. Click I Accept	After login, a Warning message will indicate that questions must be answered in order to continue.			
224			5	Click on Answer Questions button; Verify ULTRUS logo with updated Header and Footer will be displayed in the Forgotten Password Questions screen.	ULTRUS logo with updated Header and Footer will be displayed in the Forgotten Password Questions screen.			
225			6	Add answers to the required number of questions and then click continue; Verify ULTRUS logo with updated Header and Footer will be displayed in the Knowledge Center screen.	User will be navigated to the Knowledge Center and ULTRUS logo with updated Header and Footer will be displayed in the Knowledge Center screen.			
226			7	Sign out and login as Admin User mentioned in the Precondition; Click on User Profile, click on Administrative View; Click Reports; Generate the event log report for the following events: 1. Invalid Login Attempt 2. Login	Event log report for the admin user will display logs in Report time zone for the below events correctly 1. Invalid Login Attempt 2. Login			
227			8	Try to edit the above generated event log report. Verify that Admin User will not be able to edit the generated event log report.	Admin User will not be able to edit the generated event log report.			
228			9	Verify ULTRUS logo with updated Header and Footer will be displayed in the Reports screen.	ULTRUS logo with updated Header and Footer will be displayed in the Reports screen.			
229	195669	Options_Password Policies_Authentication	1	Precondition: 1. Enable e-sign requirement for password policy changes 2. Admin User				
230			2	Login as Admin user mentioned in the Precondition section.	Admin user will be able to login successfully.			
231			3	Click on User Profile, click on Administrative View.	Admin user will be navigated to Admin Home page			
232			4	Click Site Configurations, Click Password Policies.	Admin user will be navigated to Define Password Policies page.			
233			5	Click Edit Password Policies.Modify any criteria for the password policies.Click Save Changes.	Password policies will be modified and user will be required to electronically sign			

	A	B	C	D	E	F	G	H
1	**Id**	**Title**	**Test Step #**	**Test Step Description**	**Test Step Expected Result**	**Test Case Pass/ fail**	**Tester Name /Signature**	**Approval signature**
234			6	Enter user id in User ID text box. Enter password in Password text box. Verify that Password is displayed in non-readable form for e-signature.	On entering Password for e-signature, password will be displayed in non-readable form.			
235			7	Click Electronically Sign	e-signature date/timestamp will display the User's PC time zone for the current changes made to the Password Policies.			
236			8	Click Reports. Click on Event Log report and select the event "Password Policy Updated " and run the report.	The Password policy Update event will be displayed with date/time stamp based on report time zone			
237	195670	Options_PasswordPolicies _ChangePasswordLength	1	Precondition: 1. Admin User				
238			2	Login as Admin user mentioned in the Precondition section.	Admin user will be able to login successfully.			
239			3	Click on User Profile, click on Administrative View	Admin user will be navigated to Admin Home page			
240			4	Click Site Configurations, Click Password Policies.	Admin user will be navigated to Define Password Policies page.			
241			5	Click Edit Password Policies. Define Password Lengths from the drop down, selecting a number from the drop down for the "Passwords must be at least" and selecting a number for the "Passwords cannot be longer than".Click Save Changes	Minimum and maximum password lengths will be set.			
242			6	Click User profile. Click Change Password	Admin user will be navigated to Change Password page.			
243			7	Try to change your current password by entering new password and confirm new password to one with less than the minimum amount of characters required	Admin user will be unable to change the password to a length less than the minimum amount of characters required. Passwords that are shorter than the minimum lengths will return a warning message.			
244			8	Try to change your current password by entering new password and confirm new password to one that is more than the maximum amount of characters	Admin user will be unable to change the password to a length more than the maximum amount of characters. Passwords that are longer than the maximum lengths will return a warning message.			
245			9	Change your password which meets the password policy length requirements.	The user's password will be changed to a new password.			
246			10	Click Sign out and login with user id and new password.	User will Sign out and Login successfully.			
247	195671	Options_Password Policies_Password Complexity Requirement	1	Precondition: 1. Admin user				
248			2	Login as Admin User. Click on User Profile, click on Administrative View and Click Site Configuration. Click Password Policies. Click Edit Password Policies	Edit password policies page should be displayed			
249			3	Select any password complexity requirement.Click Save Changes	The password policies will be defined to require a combination of letters and/or numbers.			
250			4	Click on User profile. Click Change Password; Try to change the password to one that does not conform to the complexity rules.	When attempting to change to a nonconforming password, user will see a message indicating what the password must contain.			
251			5	Try to change the password to one that does conform to the complexity rules	When changing the password to one that does conform, the new password will be accepted and the system will respond with a message that the password has been changed.			
252			6	Change your password which meets the password policy complexity rules.	The user's password will be changed to a new password.			
253			7	Click Sign out and login with user id and new password.	User will Sign out and Login successfully.			
254	195672	Options_Password policies_Restrict reuse of	1	Precondition: 1. Admin User				

	A	B	C	D	E	F	G	H
1	**Id**	**Title**	**Test Step #**	**Test Step Description**	**Test Step Expected Result**	**Test Case Pass/ fail**	**Tester Name /Signature**	**Approval signature**
255		passwords	2	Login as an Admin user. Click on User Profile, click on Administrative View and Click on Site Configuration. Click Password Policies	Define Password Policies page should be displayed			
256			3	Click Edit Password Policies, Select option: Do not allow reuse of past '' password(s) and select a number from the drop down, Click Save Changes	The Password policies will be defined to not allow reuse of a selected number of passwords.			
257			4	Click on User Profile, click Change Password. Change the password several times, until the total # of changes at least 1 more than the # of reuses selected.	User will attempt to change password reusing his current password, until the total # of attempts is 1 more than the # of reuses selected.			
258			5	Try to change password, reusing the password immediately prior.	User will not be able to change the password.			
259			6	Repeat step 4 until total # of changes attempted is 1 more than the # of reuses selected.	When attempting the last reuse, the password will be accepted and his password will be changed.			
260	195675	Logs_Event log report_Allow Additional Quiz Attempts and Allow Additional Custom Exam Attempts	1	Precondition: 1. Admin User. 2. Control Document Training Item#1 and Custom Exam Training Item#2 with Quiz and Maximum Allowed Attempts is set. 3. Assignment for Training Item#1 to User#1 & Training Item#2 to User#2. 4. User#1 attempted Training Item#1 and failed the Quiz same # of times as the Max Attempts set ensuring User is Locked out. 5. User#2 attempted Training Item#2 and failed the Exam same # of times as the Max Attempts set ensuring User is Locked out. 6. Admin User granted additional attempt to the Locked Quiz of User#1 and Training Item#1. 7. Admin User granted additional attempt to the Locked Exam of User#2 and Training Item#2.				
261			2	Login as Admin User; Access User Profile; Click on Administrative View; Click on Reports menu and Click on " Event Log Report" link.	Event Log Report page will be displayed.			
262			3	Click on "Edit" and select "Filters" tab. Remove existing saved filters. Select "Event" as filter type, select IS operator from drop down, verify new event 'Allow Additional Quiz Attempts' will be listed in the value dropdown.Select 'Allow Additional Quiz Attempts' value in value box; Click on "+ Set Filter" buttonApply Filters to display the record for User#1 and Training Item#1 mentioned in the Precondition and Click on 'Run Report without saving'.	Record will be displayed as per the applied filter criteria in the generated Event Log report.			
263			4	Verify that the Affected Entity and Affected Entity Type are displayed as below for the Event "Allow Additional Quiz Attempts" in the generated Event Log Report.Event: 'Allow Additional Quiz Attempts' Affected Entity Type: Quiz AssignmentAffected Entity: 'User Last Name, User First Name (User ID) | Training Title (Training Code) Manjor.Minor [Type Abbr]'	Affected Entity and Affected Entity Type will be displayed as below in the generated Event Log Report. Event: 'Allow Additional Quiz Attempts' Affected Entity Type: Quiz AssignmentAffected Entity: 'User Last Name, User First Name (User ID) | Training Title (Training Code) Manjor.Minor [Type Abbr]'			
264			5	Click on "Edit" and select "Filters" tab; Select "Event" as filter type, select IS operator from drop down, verify new event 'Allow Additional Custom Exam Attempts' will be listed in the value dropdown.Select 'Allow Additional Custom Exam Attempts' value in value box; Click on "+ Set Filter" buttonApply Filters to display the record for User#2 and Training Item#2 (if necessary) mentioned in the Precondition and Click on 'Run Report without saving'.	Record will be displayed as per the applied filter criteria in the generated Event Log report.			
265			6	Verify that the Affected Entity and Affected Entity Type are displayed as below for the Event "Allow Additional Exam Attempts" in the generated Event Log Report.Event: 'Allow Additional Custom Exam Attempts' Affected Entity Type: Exam AssignmentAffected Entity: 'User Last Name, User First Name (User ID) | Training Title (Training Code) Manjor.Minor [Type Abbr]'	Affected Entity and Affected Entity Type will be displayed as below in the generated Event Log Report. Event: 'Allow Additional Custom Exam Attempts' Affected Entity Type: Exam AssignmentAffected Entity: 'User Last Name, User First Name (User ID) | Training Title (Training Code) Manjor.Minor [Type Abbr]'			
266	196288	Support_Platform documentation	1	Precondition 1. User with Learner role only				
267			2	Log on as a Learner mentioned in setup	User will be able to login successfully.			
268			3	Click on 'Support' icon--> Click platform documentation. Click on ComplianceWire Learners Guide link	ComplianceWire Learners Guide will be launched in new tab in PDF format. User will be able to view the file.			

	A	B	C	D	E	F	G	H
1	**Id**	**Title**	**Test Step #**	**Test Step Description**	**Test Step Expected Result**	**Test Case Pass/ fail**	**Tester Name /Signature**	**Approval signature**
269	310860	Training Item_Classes_Class GI Screen_Add_Edit_Copy_Remove_Disable Class	1	Precondition: 1. Admin User 2. Date/Time Format along with Time Display Settings set as Non-Military Time (hh:mm:ss tt UTC-5 (13:30:55 PM UTC-5)) or hh:mm:ss tt (13:30:55 PM) to above Admin User. 3. User#1 4. ILC Training item#1 in Effective status with Class in Enabled status.				
270			2	Login as Admin User, navigate to Admin Home, search for ILC Training item#1, click on Classes and click on Enabled Class; Click on Add Class in the left nav, enter/select data in Start Date, End Date and other mandatory fields and Click on "Save Class". Verify new Class is added and Admin User is navigated to the Class GI screen.	New Class will be added in Enabled Status and Admin User will be navigated to the Class GI screen.			
271			3	Click on Actions, click on Edit Class, update data in the Start Date, End Date and other mandatory fields and click on Save changes. Verify Admin User is able to update the Class details and navigated to the Class GI Screen.	Admin User will be able to update the Class details and navigated to the Class GI Screen.			
272			4	Click on Actions, click on Copy Class, update data in the Start Date, End Date and other mandatory fields and click on Save changes. Verify new Class is added and Admin User is navigated to the Class GI screen.	New Class will be added in Enabled Status and Admin User will be navigated to the Class GI screen.			
273			5	Click on Remove Class under Actions; Click on REMOVE button; Verify Admin User is navigated to the Classes list Screen. Apply filter for Status column to display "Removed" (If Applicable); Verify the status of the Class is changed to "Removed" Click on the Class Code; Verify the status of the Class is changed to "Removed" in the Class general Information screen.	Admin User will be navigated to the Classes list Screen. Status of the Class will be changed to "Removed" in the Classes screen and Class general Information screen.			
274			6	Click on Add Historical Class in the left nav, enter/select data in Start Date, End Date and other mandatory fields, add User#1 and Click on "Save Class". Verify new Class is added and Admin User is navigated to the Class GI screen.	New Class will be added in Enabled Status and Admin User will be navigated to the Class GI screen.			
275			7	Navigate to ILC Training Item General Information screen, Retire the ILC Training Item and click on Classes. Verify the Enabled Classes status is updated to Disabled in the grid. Click on the Disabled Class; Verify all details are displayed correctly in the Class General Information screen.	Enabled Classes status will be updated to Disabled in the grid. All details will be displayed correctly in the Class General Information screen for the Disabled Class.			
276			8	Click on Reports and generate "Event Log Report" for the below Events and verify the records are displayed correctly in the generated Event Log Report to the Admin User: 1. Add Class 2. Edit Class 3. Remove Class 4. Disabled Class	Records will be displayed correctly in the generated Event Log Report to the Admin User.			