Clearlane Tests

Protocole de qualification opérationnelle (OQ)

À dérouler dans un projet Jira de test, avec au moins deux utilisateurs de test. Noter la version de l'appli (Gérer les applis) et votre site avant de commencer. Joindre une capture à chaque test. Un projet Jira de test (clé notée KEY) avec Clearlane Tests installé et l'abonnement actif ; quatre tickets Story S1 à S4 (les seules stories du projet), un ticket Tâche E1 pour les preuves, une version « 1.0 » et un type de ticket « Bug ». Utilisateur A : administrateur du projet (Parcourir les projets, Modifier les tickets, Administrer les projets). Utilisateur B : testeur (Parcourir les projets, Modifier les tickets, Créer des tickets). Langue de Jira : français. Exécuter les tests dans l'ordre : chacun utilise les données des précédents. Les heures sont affichées dans votre fuseau à l'écran et en UTC dans le PDF.

Version de l'appli	
Site	
Exécuté par	
Date	
Approuvé par	

Test	Étapes	Résultat attendu	Résultat (conforme / non conforme)	Testeur, date
OQ-01 Mettre en place les signatures électroniques	En tant qu'utilisateur A, ouvrir « Clearlane Tests » dans la barre latérale du projet, onglet « Réglages ». Sous « Réglages du projet », choisir « Chaque exécution et la clôture » pour « Signatures électroniques », « Bug » pour « Type des bugs créés depuis une étape en échec », sélectionner « Story » dans « Types d'exigences (couverture) », cliquer sur « Enregistrer », puis sur « Historique des modifications ». Ensuite, en tant qu'utilisateur A puis B, dans « Mon mot de passe de signature », saisir un mot de passe de 5 caractères dans « Nouveau mot de passe de signature » et cliquer sur « Définir mon mot de passe de signature » ; puis saisir un mot de passe d'au moins 8 caractères et cliquer à nouveau.	« Réglages enregistrés » s'affiche et l'historique des modifications liste le changement avec le nom de l'utilisateur A, la date et l'heure. Le mot de passe de 5 caractères est refusé avec « Mot de passe trop court. » ; le mot de passe valable donne « Mot de passe de signature enregistré » et « Votre mot de passe de signature est défini. »		
OQ-02 Créer un cas de test lié à une exigence	En tant qu'utilisateur A, onglet « Cas de test », cliquer sur « Nouveau cas de test ». Saisir un « Titre » et trois étapes, chacune avec « Action », « Données de test » et « Résultat attendu » (bouton « Ajouter une étape »). Dans « Couvre (exigences) », rechercher et choisir S1. Cliquer sur « Enregistrer ». Modifier le « Résultat attendu » de l'étape 2 et cliquer à nouveau sur « Enregistrer ». Dans « Versions », cliquer sur « Voir » pour la version 1.	« KEY-T1 créé » s'affiche ; le cas indique « Version 1 », la carte « Couvre » liste S1 avec son résumé, et « Historique » montre « Création » avec le nom de l'utilisateur A, la date et l'heure. Après la modification : « Enregistré · version 2 » ; « Versions » liste les versions 1 et 2 avec auteur et date, « Voir » affiche les étapes d'origine de la version 1, et « Historique » montre « Version 2 : étapes ».		

Test	Étapes	Résultat attendu	Résultat (conforme / non conforme)	Testeur, date
OQ-03 Importer des cas de test depuis un CSV et en archiver un	Préparer un fichier CSV avec l'en-tête « Summary,Action,Expected result,Requirement » et trois lignes : « Login works,Open the sign-in page,The form is shown,[clé de S3] », « ,Enter valid credentials,The home page is shown, » et « Logout works,Click Sign out,The sign-in page is shown, ». En tant qu'utilisateur A, onglet « Cas de test », cliquer sur « Importer un CSV », choisir le fichier dans « Fichier CSV » et cliquer sur « Importer 2 cas ». Ouvrir « Logout works », mettre « Statut » à « Obsolète », cliquer sur « Enregistrer », puis sur « Archiver ». Dans la liste des cas, cliquer sur « Archives ».	Avant l'import : « Format reconnu : CSV générique · 2 cas · 3 étapes ». Après : « 2 cas importés » ; « Login works » a 2 étapes et couvre S3. Après l'archivage : « [clé du cas] archivé » ; le cas quitte la liste et figure dans « Archives », s'ouvre avec « Archivé : hors de la bibliothèque et de la limite de cas, gardé avec son historique. » et son « Historique » montre « Archivage ».		
OQ-04 Panneau du ticket	En tant qu'utilisateur A, ouvrir la story S2 dans Jira et ouvrir le panneau « Clearlane Tests ». Cliquer sur « + Nouveau cas de test », saisir un « Titre » et, dans « Étapes », deux lignes : « Ouvrir la page des commandes = › La commande est listée » et « Cliquer sur Payer = › Commande confirmée » ; cliquer sur « Enregistrer ». Cliquer sur « Lier un cas », saisir KEY-T1 et cliquer sur « Lier un cas » ; puis cliquer sur « Délier » à côté de KEY-T1.	Avant : « Couverture » indique « Non couvert » et « Aucun cas de test ne couvre encore ce ticket. » Après l'enregistrement : « [clé du cas] créé » ; le cas est listé avec « Non exécuté », le panneau indique « 1 cas de test » et la couverture « Non exécuté ». La liaison donne « KEY-T1 lié » et le liste ; « Délier » donne « KEY-T1 délié » et le retire. Un clic sur le nouveau cas l'ouvre dans Tests, avec S2 sous « Couvre » et 2 étapes.		
OQ-05 Créer une campagne et assigner les exécutions	En tant qu'utilisateur A, onglet « Campagnes », cliquer sur « Nouvelle campagne ». Saisir un « Titre », choisir « 1.0 » dans « Version », une « Échéance » et E1 dans « Ticket Jira des preuves » ; cliquer sur « Enregistrer ». Cliquer sur « Ajouter des cas », cocher KEY-T1, le cas créé depuis S2 et « Login works », choisir l'utilisateur B dans « Rechercher une personne » et cliquer sur « Ajouter 3 cas ». Puis, en tant qu'utilisateur B, ouvrir « Clearlane Tests » depuis le menu Applications de Jira.	« KEY-C1 créée » ; l'en-tête affiche KEY-C1 · 1.0 et l'échéance. Après l'ajout : « 3 cas ajoutés » ; trois exécutions, chacune « Non exécuté », avec l'utilisateur B dans « Assigné à », et « Exécutions » = 3. L'utilisateur B voit les trois exécutions sous « Exécutions qui vous sont assignées », avec la campagne et l'échéance. L'« Historique » de la campagne (bouton « Ouvrir ») montre « Création » et « 3 cas ajoutés » avec le nom de l'utilisateur A.		
OQ-06 Exécuter : réussite, échec avec note, bug en un clic	En tant qu'utilisateur B, ouvrir KEY-C1 et cliquer sur l'exécution de KEY-T1 ; cliquer sur « Réussi » aux étapes 1 et 2 en moins d'une seconde en regardant l'état en haut de l'exécution, attendre 2 secondes, puis cliquer sur « Réussi » à l'étape 3. Cliquer sur « Suivant » jusqu'à l'exécution du cas créé depuis S2 : cliquer sur « Réussi » à l'étape 1 puis aussitôt sur « Retour à KEY-C1 », et rouvrir cette exécution. Cliquer sur « Échec » à l'étape 2, saisir une note dans le champ de commentaire sous l'étape 2 et cliquer en dehors. Cliquer sur « + Créer un bug », garder le « Résumé » proposé et le type « Bug », cliquer sur « Créer un bug ». Ouvrir le nouveau bug dans Jira.	KEY-T1 : après les étapes 1 et 2, « Enregistrement… », puis « Enregistré » environ 1,5 s après le dernier clic ; l'étape 3 (le résultat final) est enregistrée aussitôt : « Enregistré », résultat « Réussi », « Exécuté par [utilisateur B] · [date, heure] ». Deuxième exécution : la page de la campagne ne s'ouvre qu'une fois l'étape 1 enregistrée, et l'exécution rouverte montre l'étape 1 « Réussi » et « En cours » ; « Échec » à l'étape 2 est enregistré aussitôt (« Enregistré » sans attente). Résultat « En échec », « [clé du bug] créé et lié », et la carte « Bugs » liste le bug avec « Étape 2 ». Dans Jira, la description du bug commence par « Trouvé par Clearlane Tests : [clé du cas] (version 1) dans la campagne KEY-C1. » et donne les étapes pour reproduire, le résultat attendu de l'étape 2 et « Obtenu : » avec la note ; le bug est lié à S2 et son panneau « Clearlane Tests » affiche « Trouvé par » « KEY-C1 · [clé du cas] · étape 2 ». La campagne indique 1 « Réussies », 1 « En échec », 1 « Non exécutées » et un « Taux de réussite » de 50 %.		

Test	Étapes	Résultat attendu	Résultat (conforme / non conforme)	Testeur, date
OQ-07 Couverture des exigences (traçabilité)	En tant qu'utilisateur A, onglet « Couverture » : garder le projet de test dans « Exigences du projet », vérifier que seul « Story » est sélectionné dans « Types de tickets » (repris des réglages du projet), garder « Dernier résultat » dans « Résultats », cliquer sur « Afficher la couverture ». Cliquer sur le compteur « Non couvert », puis à nouveau. Cliquer sur « Exporter en CSV ». Dans la recherche de tickets Jira, lancer la requête JQL testCoverage = failed.	« 4 exigences » et « 75 % couverts » ; S1 « Réussi » (KEY-T1), S2 « En échec » (son cas), S3 « Non exécuté » (« Login works »), S4 « Non couvert » sans cas ; chaque clé de cas est colorée selon son résultat et ouvre le cas. Le compteur « Non couvert » filtre le tableau sur S4. Le fichier KEY-coverage.csv a les colonnes Requirement, Summary, Type, Jira status, Coverage, Test cases (en-têtes en anglais), chaque clé de cas suivie de son résultat. La requête JQL renvoie S2.		
OQ-08 Signer une exécution : mauvais mot de passe et blocage	En tant qu'utilisateur A, ouvrir l'exécution de KEY-T1 dans KEY-C1. En tant qu'utilisateur B, ouvrir la même exécution ; dans « Signer cette exécution », saisir un mauvais mot de passe dans « Mot de passe de signature actuel » et cliquer sur « Signer cette exécution » ; recommencer avec de mauvais mots de passe jusqu'à ce que le message change, puis essayer le bon. Attendre la fin du blocage (15 minutes par défaut, « Blocage (minutes) » dans « Réglages du site (administrateurs Jira) ») et signer avec le bon mot de passe.	L'utilisateur A voit « Seule la personne qui a enregistré le résultat le signe. » et aucun champ de mot de passe. Utilisateur B : les mauvais mots de passe 1 à 4 donnent « Mot de passe de signature incorrect. » ; le 5e (valeur par défaut d'« Essais avant blocage ») donne « Signature bloquée quelques minutes après trop d'essais. », et le bon mot de passe est refusé avec le même message pendant le blocage. Après le blocage : « Exécution signée » ; la carte affiche « Signée par [utilisateur B] le [date, heure] », la déclaration « J'ai exécuté KEY-T1 (version 2) dans la campagne KEY-C1, et les résultats enregistrés reflètent fidèlement cette exécution. » et « SHA-256 » suivi de 64 caractères hexadécimaux ; la campagne affiche « ✓ Signée » sur l'exécution et son « Historique » montre « KEY-T1 signé ».		
OQ-09 Clôture signée d'une campagne	En tant qu'utilisateur A, ouvrir KEY-C1, cliquer sur « Clôturer la campagne », saisir le bon mot de passe et cliquer sur « Clôturer la campagne ». Puis, en tant qu'utilisateur B, signer l'exécution en échec comme au test 8. En tant qu'utilisateur A, cliquer sur « Clôturer la campagne », saisir un mauvais mot de passe et confirmer ; puis saisir le bon mot de passe et confirmer. Noter la valeur SHA-256 affichée.	La première tentative est refusée avec « Des exécutions faites ne sont pas encore signées. » (la campagne affiche aussi « 1 exécution faite pas encore signée : chaque testeur signe avant la clôture. »). Le cadre affiche « La clôture fige tous les résultats de la campagne. Les exécutions non faites sont signalées comme non exécutées. » et la déclaration « J'approuve les résultats de la campagne KEY-C1 (3 exécutions : …) et je la clôture. » avec les nombres. Mauvais mot de passe : « Mot de passe de signature incorrect. » et la campagne reste « Ouverte ». Bon mot de passe : « KEY-C1 clôturée », statut « Clôturée », « Clôturée par [utilisateur A] le [date, heure] », la déclaration, « Signature de clôture valide : les résultats sont ceux qui ont été signés. » et « SHA-256 » suivi de 64 caractères hexadécimaux ; l'« Historique » montre « Clôture signée ».		
OQ-10 Résultats figés après la clôture ; réouverture	En tant qu'utilisateur B, ouvrir l'exécution en échec de KEY-C1 et essayer de changer le résultat d'une étape. En tant qu'utilisateur A, cliquer sur « Rouvrir », saisir « abc » et cliquer sur « Rouvrir » ; puis saisir un motif d'au moins 5 caractères et cliquer sur « Rouvrir ». En tant qu'utilisateur B, passer l'étape 2 de cette exécution à « Réussi » et signer de nouveau l'exécution ; en tant qu'utilisateur A, clôturer de nouveau la campagne avec le mot de passe de signature.	Pendant la clôture : l'exécution affiche « Cette campagne est clôturée : les résultats sont figés. », ses boutons de résultat sont désactivés, et « + Créer un bug », « Lier un bug existant », « Joindre des fichiers », « Ajouter des cas », « Modifier » et « Clôturer la campagne » ne sont pas proposés ; l'utilisateur B n'a pas « Rouvrir ». « abc » est refusé avec « Indiquez un motif (au moins 5 caractères). » ; le motif donne « KEY-C1 rouverte » et l'« Historique » montre « Réouverture : [motif] ». Après le changement, l'exécution est « Réussi », sa signature a disparu (« Ce projet signe chaque exécution faite. ») et l'« Historique » montre « [clé du cas] : En échec → Réussi », « [clé du cas] : résultats enregistrés modifiés : étape 2 : En échec → Réussi » et « [clé du cas] : signature annulée (résultats modifiés) ». La nouvelle clôture affiche une valeur SHA-256 différente de celle notée au test 9.		

Test	Étapes	Résultat attendu	Résultat (conforme / non conforme)	Testeur, date
OQ-11 Rapport PDF, piste d'audit et archivage	En tant qu'utilisateur A, ouvrir KEY-C1, cliquer sur « Rapport PDF » et ouvrir le fichier téléchargé KEY-C1-report.pdf ; le comparer à la page de la campagne et à son « Historique » (bouton « Ouvrir »). Puis cliquer sur « Archiver », revenir à « Campagnes », cliquer sur « Archives », ouvrir KEY-C1 et cliquer de nouveau sur « Rapport PDF ».	Le PDF « Rapport de campagne de tests » affiche KEY-C1 et son titre ; Statut, Version 1.0, Échéance, Créée et Clôturée (date, heure UTC, nom), Ticket des preuves E1 ; « Synthèse » ; « Couverture des exigences (dans cette campagne) » ; « Résultats » (Cas, Titre, Vers., Résultat, Exécuté par, Date (UTC), Bugs, Signé) ; « Signatures électroniques » (Objet, Nom, Date (UTC), Déclaration, Empreinte SHA-256, « Résultats identiques à ceux signés. ») pour la clôture et chaque exécution signée, avec l'empreinte de clôture affichée à l'écran ; « Enregistrements d'exécution » avec l'action, les données, le résultat attendu, le résultat et le commentaire de chaque étape (« Non exécuté. » pour l'exécution non faite) ; « Piste d'audit » avec chaque événement de l'historique, dont le motif de réouverture, le résultat d'étape modifié et la signature annulée ; « Généré le [date] par [utilisateur A] · Clearlane Tests » et « Page x / y » sur chaque page. Après l'archivage : « KEY-C1 archivée » ; la campagne n'est plus listée que dans « Archives », s'ouvre avec « Archivée : hors de la liste et de la limite de campagnes, gardée avec son rapport. » et son rapport PDF peut toujours être généré.		
OQ-12 L'accès suit les permissions Jira	En tant qu'utilisateur A, ouvrir KEY-T1 depuis « Clearlane Tests » (menu Applications de Jira) et copier l'adresse du navigateur. Retirer à l'utilisateur B la permission « Parcourir les projets » sur le projet de test (par exemple en le retirant du rôle du projet). En tant qu'utilisateur B, ouvrir « Clearlane Tests » depuis le menu Applications, puis l'adresse copiée. En tant qu'utilisateur A, créer une campagne KEY-C2, cliquer sur « Ajouter des cas », cocher KEY-T1, choisir l'utilisateur B dans « Rechercher une personne » et cliquer sur « Ajouter 1 cas ». Rendre ensuite la permission à B.	L'utilisateur B ne voit ni le projet sous « Projets avec des tests » ni aucune de ses exécutions sous « Exécutions qui vous sont assignées » ; l'adresse copiée affiche « Introuvable, ou dans un projet que vous ne voyez pas. » et aucune donnée de test. L'assignation à l'utilisateur B est refusée avec « Cette personne ne voit pas le projet : choisissez quelqu'un qui le voit. »		