Bring Your Own Key (BYOK) - Guide de l'utilisateur

Version 8 du document

Sommaire

Bring Your Own Key (BYOK) 1
Comment BYOK protège vos données 2
Pratiques recommandées 3
Espaces de travail de développement 3
S'assurer que les espaces de travail ne sont pas utilisés 3
Chiffrement avant le chargement des données 3
Identification des utilisateurs à assigner aux rôles clef 3
Rôle d'administrateur du chiffrement (Encryption Admin) 4
Rôle d'auditeur du locataire (Tenant Auditor) 4
Attente 4
Prise en main de BYOK 5
1) Choisissez un administrateur du chiffrement 5
2) Ajoutez l'utilisateur doté du rôle d'administrateur du chiffrement à l'espace de travail ... 5
3) Demandez l'assignation du rôle d'administrateur du chiffrement 6
4) Accédez à BYOK dans Anaplan Administration 6
Génération ou téléchargement de vos clés de chiffrement 8
Génération et téléchargement de clés symétriques 8
Utilisation de clés encapsulées 10
Génération et exportation d'une clé asymétrique 11
Encapsulation de la clé symétrique à l'aide de la clé asymétrique 13
Remarque : Anaplan ignore tout autre contenu de la charge utile encapsulée. 14
Importation de la clé encapsulée 14
Désactivation d'une clé de chiffrement 18
Activation d'une clé de chiffrement 19
Rappel associé aux clés 20
Modification de la date de rappel d'une clé 20
Chiffrement d'un espace de travail à l'aide de l'une de vos clés de chiffrement 22
Considérations à prendre en compte lors d'un chiffrement initial 22
Affectation d'une clé à un espace de travail 22
Espaces de travail ayant l'état (State) Ready (Prêt) 24
Déchiffrement d'un espace de travail 25
Rotation des clés 27
Affichage de l'historique des clés 29
Recherche d'une clé de chiffrement 30
Notifications relatives aux événements de chiffrement 31

© Anaplan 2018

Quelles sont les données chiffrées par BYOK ? **32**
Glossaire des événements et termes de chiffrement **33**
Enable Support Access (Activer l'accès support) **35**
Activation de l'accès à partir d'une demande de l'équipe de support 35
Activation de l'accès sans demande de l'équipe de support 36
Disable Support Access (Désactiver l'accès support) 37
Affichage de l'accès support 38
Journaux d'audit **39**
Glossaire des événements de chiffrement **40**

 © Anaplan 2018

Bring Your Own Key (BYOK)

Anaplan sait que vos données font partie de vos actifs les plus importants. C'est à vous qu'elles appartiennent et nous n'y accédons jamais sans votre autorisation préalable. Pour plus d'informations sur la sécurité de nos données et de notre plateforme, rendez-vous sur trust.anaplan.com.

L'application Bring Your Own Key (BYOK) vous permet maintenant de vous approprier les clés de chiffrement de vos données de modèle. Si vous avez accès à l'outil Anaplan Administration (https://community.anaplan.com/anapedia/tenant-administration/accessing-the-administration-tool), vous pouvez chiffrer et déchiffrer des espaces de travail sélectionnés à l'aide de vos propres clés AES-256. À la différence des clés principales système, les clés créées par BYOK vous appartiennent et vous en assurez la sécurité. Aucun mécanisme ne permet au personnel Anaplan d'accéder à vos clés.

Si vous décidez de mettre en œuvre BYOK, vos clés sont hébergées par Anaplan et stockées dans un gestionnaire de clés. Un gestionnaire de clés est un dispositif physique qui protège les clés contre les accès non autorisés, les cyber-attaques et les intrusions physiques. Les clés sont gérées par un ou plusieurs utilisateurs internes auxquels a été assigné le rôle d'administrateur du chiffrement. Une fois les clés générées dans Administration (ou téléchargées depuis une application de gestion cryptographique), l'administrateur du chiffrement affecte une clé à un espace de travail pour chiffrer tous les modèles qu'il contient. Dans un espace de travail chiffré par BYOK, les données de modèles sont chiffrées au repos, mais non lorsqu'elles sont chargées en mémoire.

> ***Remarque :*** *Bring Your Own Key (BYOK) est un produit complémentaire que votre organisation peut acheter si elle possède l'édition Enterprise.*

© Anaplan 2018

Comment BYOK protège vos données

La mise en œuvre de BYOK assure la prise en charge de vos objectifs de sécurité informatiques, en particulier les programmes de gouvernance des données, les plans de reprise d'activité et la conformité à la législation en vigueur.

© Anaplan 2018

Pratiques recommandées

Cette section passe en revue diverses pratiques recommandées à appliquer lorsque vous utilisez BYOK.

Espaces de travail de développement

1. Identifiez ou créez un espace de travail qui ne contient aucune donnée de modèle stratégique.
2. Chiffrez l'espace de travail pour vous habituer à utiliser BYOK.
3. Une fois l'espace de travail chiffré :
   a. Exécutez les tests requis sur les modèles de l'espace de travail chiffré.
   b. Suivez la même procédure pour chiffrer l'espace de travail de production.
   c. Le cas échéant, déchiffrez l'espace de travail de développement.

S'assurer que les espaces de travail ne sont pas utilisés

Il est impossible de chiffrer un espace de travail actif. Avant de démarrer le chiffrement, assurez-vous que les utilisateurs n'utilisent plus les modèles que contient l'espace de travail. Ne démarrez pas le chiffrement tant que l'espace de travail n'a pas l'état (State) « Ready » (Prêt).

Chiffrement avant le chargement des données

Le chiffrement initial porte le nom de chiffrement « in place » (là où résident les données et sans réorganisation de ces dernières) et est effectué hors ligne. Pour réduire le temps que prend ce chiffrement, nous vous recommandons de chiffrer un espace de travail lorsqu'il vient d'être créé ou avant le chargement de données stratégiques. Les données ajoutées aux modèles que contient l'espace de travail après le chiffrement sont automatiquement chiffrées. Ce processus porte le nom de « chiffrement à la volée ». Ces données sont probablement sensibles et il est plus sûr de les charger après le chiffrement de l'espace de travail.

Identification des utilisateurs à assigner aux rôles clef

Identifiez dès que possible les utilisateurs auxquels sera assigné le rôle d'administrateur du chiffrement (Encryption Admin).

 © Anaplan 2018

Identifiez les utilisateurs auxquels sera assigné le rôle d'auditeur du locataire (Tenant Auditor).

Rôle d'administrateur du chiffrement (Encryption Admin)

Pour assurer la séparation des tâches, un administrateur du chiffrement ne devrait avoir accès à aucune donnée de modèle.

- Assurez-vous que les administrateurs du chiffrement appartiennent à un espace de travail au moins et que l'autorisation de modèle « No Access » (Aucun accès) leur a été assignée.
- Communiquez à votre chargé de compte l'adresse e-mail des administrateurs du chiffrement lorsque vous commandez BYOK.
- Assignez idéalement à plusieurs personnes le rôle d'administrateur du chiffrement.
- Un utilisateur doté du rôle d'administrateur du chiffrement (Encryption Admin) peut assigner à d'autres utilisateurs de son locataire le rôle d'administrateur du chiffrement ou annuler son affectation à l'aide de la fonction Access Control (Contrôle d'accès) de l'application Administration. Voir Affectation du rôle d'administrateur du chiffrement.

Remarque : *le rôle d'administrateur du chiffrement (Encryption Admin) ne peut être assigné qu'à un groupe restreint d'utilisateurs. Seuls les utilisateurs figurant sur la liste d'administrateurs potentiels du chiffrement communiquée à Anaplan sont recensés à la section Access Control (Contrôle d'accès) de l'application Administration. S'il manque des utilisateurs, ajoutez-les à l'espace de travail de votre locataire dotés du rôle No Access (Aucun accès), puis contactez l'équipe de support Anaplan et demandez-lui d'ajouter ces utilisateurs à la liste des administrateurs du chiffrement éligibles.*

Rôle d'auditeur du locataire (Tenant Auditor)

Le rôle d'auditeur du locataire est autorisé à accéder aux journaux d'audit BYOK. Il est préférable, mais pas obligatoire, de sélectionner des utilisateurs auxquels vous n'avez pas également assigné le rôle d'administrateur du chiffrement. L'administrateur client (Tenant Administrator) peut assigner des utilisateurs à ce rôle. Un auditeur du locataire doit être un utilisateur dans un espace de travail Anaplan au moins et doit idéalement posséder l'autorisation de modèle « No Access » (Aucun accès).

Attente

Lorsque l'état « BYOK » change suite à une opération de chiffrement ou de déchiffrement dans un espace de travail, attendez deux minutes avant d'exécuter une autre opération dans cet espace de travail. Les processus en cours peuvent ainsi se terminer et vous évitez les erreurs inattendues.

 © Anaplan 2018

Prise en main de BYOK

Si vous êtes convaincu que BYOK répond à vos besoins de sécurité, procédez comme suit pour démarrer la prise en main.

1) Choisissez un administrateur du chiffrement

Commencez par désigner un administrateur du chiffrement de votre locataire. Un administrateur du chiffrement gère les clés de chiffrement, mais n'a accès ni aux espaces de travail, ni aux modèles. Choisissez un collaborateur chargé de la sécurité informatique, mais qui n'utilise pas Anaplan (y compris via l'interface de programmation applicative) dans le cadre de ses attributions. Vous devez choisir au moins un administrateur du chiffrement pour le locataire.

2) Ajoutez l'utilisateur doté du rôle d'administrateur du chiffrement à l'espace de travail

ADMINISTRATEURS D'ESPACE DE TRAVAIL UNIQUEMENT

Dans l'espace de travail à chiffrer, vous devez ajouter l'administrateur du chiffrement à titre d'utilisateur sans accès aux modèles.

1. Dans Anaplan, ouvrez n'importe quel modèle de l'espace de travail à chiffrer.
2. Accédez à **Settings (Paramètres) > Users (Utilisateurs).**
3. Cliquez sur **Add User (Ajouter un utilisateur)**. La boîte de dialogue Add User (Ajouter un utilisateur) s'affiche.
4. Renseignez les champs **Email Address (Adresse e-mail)**, **First Name (Prénom)** et **Last Name (Nom)** relatifs au nouvel utilisateur.
5. Pour garantir la séparation des tâches, NE cochez PAS les cases Workspace Admin (Administrateur d'espace de travail) et Authentication with Single Sign-on (Connexion par authentification unique).
6. Dans la liste **Role (Rôle)**, sélectionnez No Access (Aucun accès).
7. Cliquez sur OK.

Répétez cette procédure pour chaque administrateur du chiffrement à désigner.

Si l'administrateur du chiffrement désigné existe déjà en tant qu'utilisateur dans l'espace de travail à chiffrer, assignez-lui l'attribut « No Access (Aucun accès) » dans Model Role (Rôle du modèle).

Pour plus d'informations, consultez Users (Utilisateurs) (https://community.anaplan.com/anapedia/around-the-platform/settings-tab/users).

© Anaplan 2018

3) Demandez l'assignation du rôle d'administrateur du chiffrement

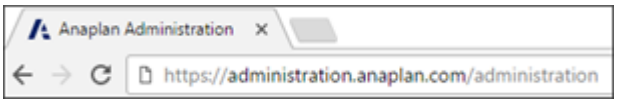
Contactez le membre de l'équipe de support Anaplan qui vous a été assigné et communiquez-lui les détails des utilisateurs qui feront office d'administrateurs du chiffrement. Vous devez désigner l'administrateur du chiffrement initial. Tout autre utilisateur proposé figurera dans Access Control (Contrôle d'accès), mais l'administrateur du chiffrement initial devra leur assigner ce rôle.

4) Accédez à BYOK dans Anaplan Administration

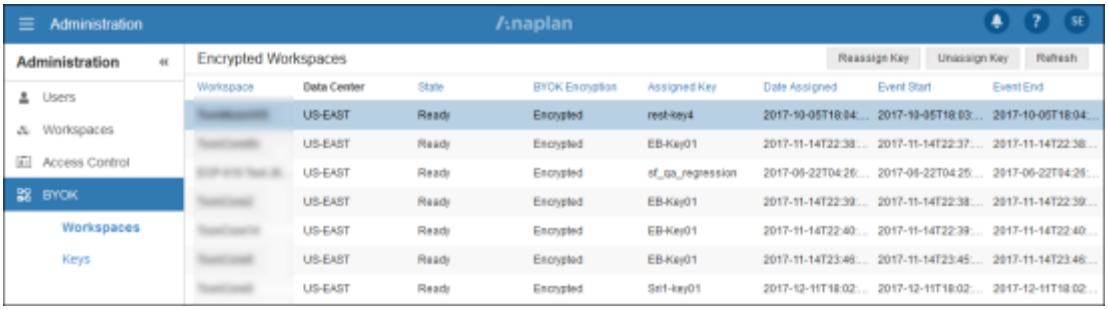
ADMINISTRATEURS DU CHIFFREMENT UNIQUEMENT

Pour accéder à BYOK dans Anaplan Administration, procédez comme suit :

1. Connectez-vous en entrant vos coordonnées d'identification standard.
2. Pour accéder à BYOK, procédez comme suit :
   a. Collez cette URL dans la barre d'adresses du navigateur : https://administration.anaplan.com/administration



   b. Cliquez sur **BYOK** dans l'encadré Anaplan Administration pour développer le menu **BYOK**. Les options **Workspaces** (Espaces de travail) et **Keys** (Clés) s'affichent alors :



   c. Selon l'option requise, cliquez sur **Workspaces** (Espaces de travail) ou **Keys** (Clés).

> ***Remarque :*** *si BYOK ne figure pas dans l'encadré Anaplan Administration, le rôle d'administrateur du chiffrement n'a peut-être pas été assigné à l'utilisateur.*

Pour retourner aux fonctions non-BYOK, supprimez byok/workspaces en fin d'URL.

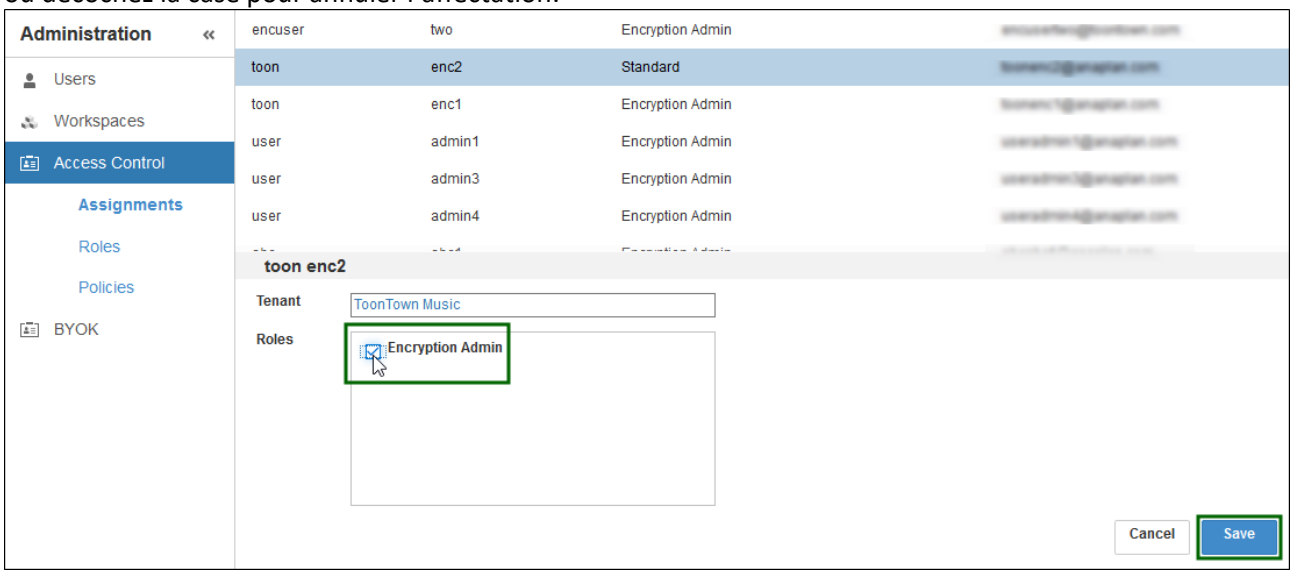
Les colonnes Event Start (Début d'événement) et Event End (Fin d'événement) s'affichent lorsqu'un événement de chiffrement d'un espace de travail démarre et prend fin. Un événement de chiffrement démarre lorsque vous affectez une clé de chiffrement. Lorsqu'un événement de chiffrement prend fin, l'espace de travail correspondant est chiffré.

 © Anaplan 2018

Affectation du rôle d'administrateur du chiffrement

En tant qu'administrateur du chiffrement, vous pouvez assigner à d'autres utilisateurs de votre locataire le rôle d'administrateur du chiffrement ou vous pouvez annuler une affectation existante. Pour ce faire, procédez comme suit:

1. Dans l'encadré Anaplan Administration, sous BYOK, sélectionnez **Access Control** (Contrôle d'accès), puis **Assignments** (Affectations).
2. Sélectionnez l'utilisateur auquel vous voulez assigner le rôle d'administrateur du chiffrement ou dont vous voulez annuler l'affectation.
3. Cochez la case **Encryption Admin** (Administrateur du chiffrement) pour assigner le rôle correspondant ou décochez la case pour annuler l'affectation.



4. Cliquez sur **Save** (Enregistrer).

© Anaplan 2018

Génération ou téléchargement de vos clés de chiffrement

ADMINISTRATEURS DU CHIFFREMENT UNIQUEMENT

En tant qu'administrateur du chiffrement, vous pouvez :

- générer des clés de chiffrement directement depuis le dispositif de gestion des clés ;
- télécharger des clés générées par une application de gestion cryptographique externe.
- télécharger une clé encapsulée.

Les clés générées en externe doivent utiliser l'algorithme de chiffrement AES (256 bits), être symétriques et être converties au format hexadécimal. La clé encapsulée doit utiliser une clé asymétrique générée par Anaplan et son format est le suivant :

Valeur secrète: (clé encapsulée en codage base 64)

Remarque : la clé asymétrique doit se terminer par un retour chariot (0d 0a).

Exemple :

Valeur secrète: VGhpcyBpcyBteSBicmFuZCBuZXcgd3JhcHBlZCBrZXk=

Anaplan ignore tout autre contenu de la charge utile encapsulée.

L'emplacement géographique auquel se réfère une clé est indiqué dans la colonne Data Center (Centre de données).

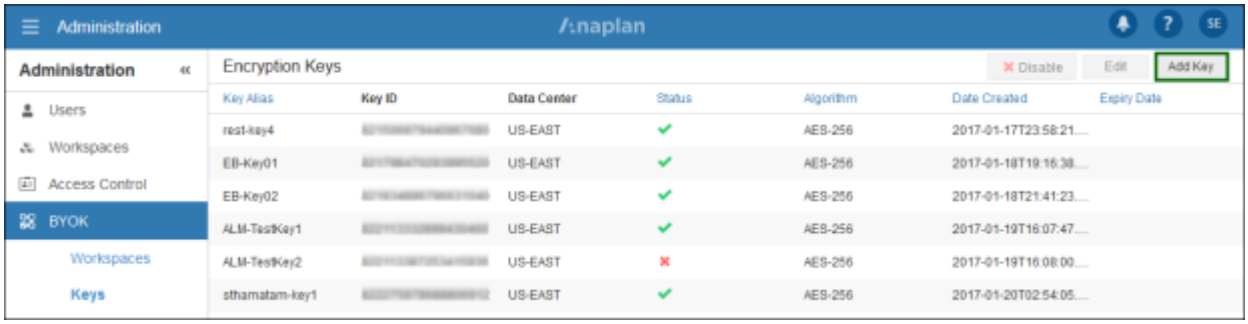
Lorsque vous générez ou que vous téléchargez une clé, elle est créée dans une région géographique déterminée et ne fonctionne que dans cette région. Si, par exemple, les données à chiffrer sont situées dans l'Union européenne, les clés de chiffrement associées à ces données sont créées dans l'Union européenne. Les clés de chiffrement ne fonctionnent que dans la région à laquelle appartiennent les données et ne sont pas synchronisées avec d'autres régions.

Génération et téléchargement de clés symétriques

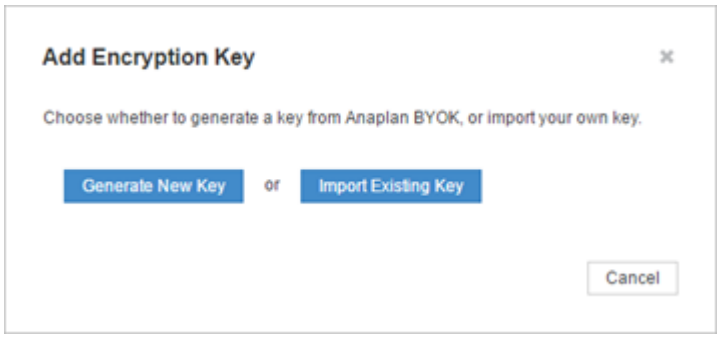
Pour générer ou télécharger des clés :

1. Dans l'encadré Anaplan Administration, sous BYOK, sélectionnez **Keys** (Clés).
2. Cliquez sur **Add Key** (Ajouter une clé).

 © Anaplan 2018



La boîte de dialogue Add Encryption Key (Ajouter une clé de chiffrement) s'affiche.



3. Pour générer une clé, cliquez sur **Generate New Key** (Générer une nouvelle clé). Dans le cas contraire, passez à l'étape 5.
   a. Affectez un alias (c'est-à-dire un nom qui vous permettra de l'identifier ultérieurement) à la clé.

> ***Remarque :*** *l'alias de la clé :*
>
> - *ne doit pas dépasser 40 caractères alphanumériques ;*
> - *doit débuter par une lettre ;*
> - *ne doit comporter ni espace, ni l'un des caractères suivants : ?:;|!@#$%^&*<=>+(){}~,\/[]'".*

   b. Le cas échéant, modifiez la date de rappel (Reminder Date).

 © Anaplan 2018

c. Cliquez sur **Generate Key** (Générer la clé).

4. Pour télécharger une clé générée en externe dans un format compatible, cliquez sur Import Existing Key (Importer une clé existante). La clé doit être au format AES-256 et symétrique.

   Dans la boîte de dialogue Import Existing Encryption Key (Importer une clé de chiffrement existante), procédez comme suit :

   a. Entrez l'alias de la clé à télécharger.

   b. Collez la clé au format hexadécimal dans le champ Hex Key (Clé au format hexadécimal). Le champ Data Center (Centre de données) n'est pas disponible.

   c. Le cas échéant, modifiez la date d'expiration (Expiration Date).

   d. Cliquez sur **Import Key** (Importer une clé).

Un identifiant unique est affecté à la clé que vous avez générée ou téléchargée. Pour visualiser la clé, accédez à BYOK > Keys (Clés).

Lorsque vous disposez d'un nombre suffisant de clés pour les espaces de travail à chiffrer, vous êtes prêt à démarrer l'affectation de clés à ces derniers.

Utilisation de clés encapsulées

Pour renforcer la sécurité, Anaplan prend en charge la génération et l'exportation de clés utilisées par l'encapsulation de clés asymétriques.

Le processus est le suivant :

1. Générez et exportez une clé asymétrique que vous pourrez utiliser ultérieurement pour encapsuler votre clé symétrique. Voir Création et exportation d'une clé asymétrique ci-après.

 © Anaplan 2018

2. Générez une clé symétrique AES-256 dans votre module HSM (Hardware Security Module, module de sécurité matériel). Étant donné que ce processus est spécifique à votre équipement, exécutez cette étape en dehors d'Anaplan.

3. Encapsulez la clé symétrique à l'aide de la clé asymétrique. Étant donné que ce processus est spécifique à votre équipement, exécutez cette étape en dehors d'Anaplan.

4. Importez la clé encapsulée dans Anaplan. Voir Importation de la clé encapsulée ci-après.

Génération et exportation d'une clé asymétrique

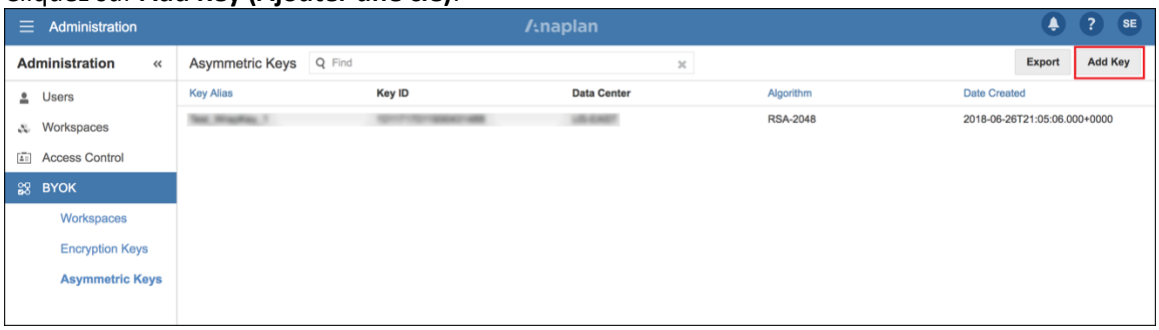
ADMINISTRATEURS DU CHIFFREMENT UNIQUEMENT

Remarque : ce processus exporte une clé publique RSA standard.

Pour créer et exporter une clé asymétrique, procédez comme suit :

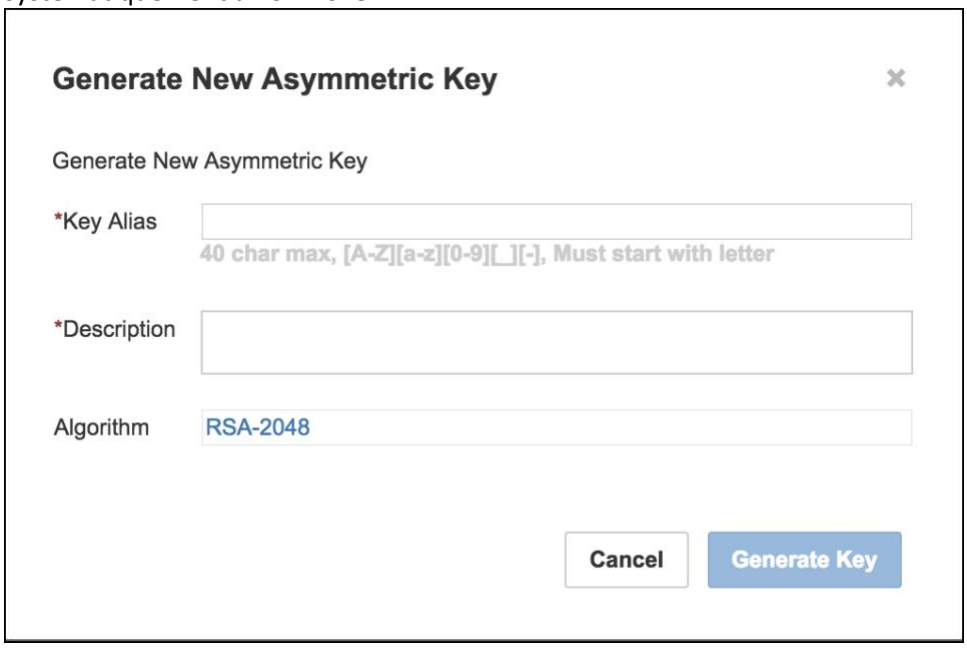
1. Dans l'encadré Anaplan Administration, sous BYOK, sélectionnez **Asymmetric Keys (Clés asymétriques)**.

2. Cliquez sur **Add Key (Ajouter une clé)**.



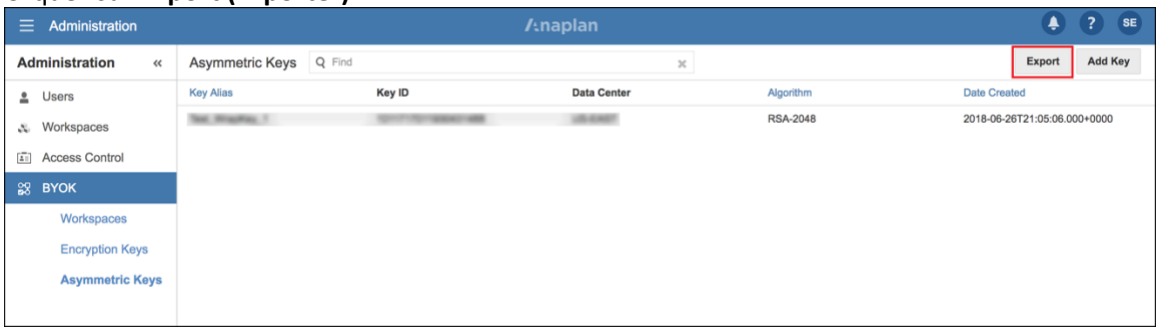
 © Anaplan 2018

3. Affectez un nom à la clé et entrez une description. L'algorithme de génération de clé correspond systématiquement à RSA-2048.



4. Sélectionnez la clé à exporter.

5. Cliquez sur **Export (Exporter)**.



 © Anaplan 2018

6. Dans la boîte de dialogue Save File (Enregistrer le fichier), cliquez sur **Save (Enregistrer)**.

Encapsulation de la clé symétrique à l'aide de la clé asymétrique

Cette procédure est exécutée par le client en dehors d'Anaplan.

1. Générez une clé symétrique AES-256 dans votre module HSM (Hardware Security Module, module de sécurité matériel).
2. Utilisez votre module HSM pour encapsuler la clé symétrique à l'aide de la clé asymétrique exportée d'Anaplan.
3. Utilisez le schéma de remplissage RSA-OAEP pour encapsuler la clé.
4. Réglez l'algorithme de remplissage avec hachage sur SHA256, SHA384 ou SHA512.
5. Réglez le générateur de masque sur SHA256, SHA384 ou SHA512.
6. Une fois la clé encapsulée, assurez-vous qu'elle est codée au format base64.
7. Créez un fichier texte et entrez les informations suivantes :

Informations à entrer	Valeur	Description
HashAlgo:	SHA256, SHA384 ou SHA512	(Facultatif) Générateur de masque utilisé dans le module HSM. Si aucune valeur n'est spécifiée, la

 © Anaplan 2018

		valeur par défaut correspond à SHA256.
MaskGenHashAlgo:	SHA256, SHA384 ou SHA512	(Facultatif) Algorithme de remplissage avec hachage utilisé dans le module HSM. Si aucune valeur n'est spécifiée, la valeur par défaut correspond à SHA256.
Secret:	(Clé encapsulée en codage base 64)	Votre clé encapsulée. Si vous n'avez spécifié ni algorithme de remplissage avec hachage ni générateur de masque, *Secret:* doit figurer en haut de page.

8. Enregistrez les modifications. Vous téléchargerez ce fichier vers Anaplan dans le cadre de la procédure Importation de la clé encapsulée ci-dessous.

Exemple (texte avec retour automatique à la ligne à des fins d'affichage uniquement)
Secret:
tlPE23P3jlxPHniXYYTr32NP0XY761NYhknIbY0H1s2yTxDFmIDBJbLJgJzC7PUAh6vgXMw+/FJ1TpZ0chl6SsEenj0WANc0qlf9XHI2205g96YZ2A2hBOTn0kGjdY9BLhbNPQZoLFq/LlVFZWXQmjSio02oGfQFyFcwNpnmKGlHtZg3zASpaEaOc0Qba2hQBoUS6aJb5/02fqhzOkAjpVU+NRmaRkS8KY5ObutDtmftwuTvguBNCBqVF1HVHGKkJz70/mQO4dHoL4T97URyDs2xtGesrJM2GVGv6CENU5CdukimdZznrq6aIYumvKPMdr/8DBKDVTbQBzVfjBL7Hg==

Remarque : Anaplan ignore tout autre contenu de la charge utile encapsulée.

Importation de la clé encapsulée

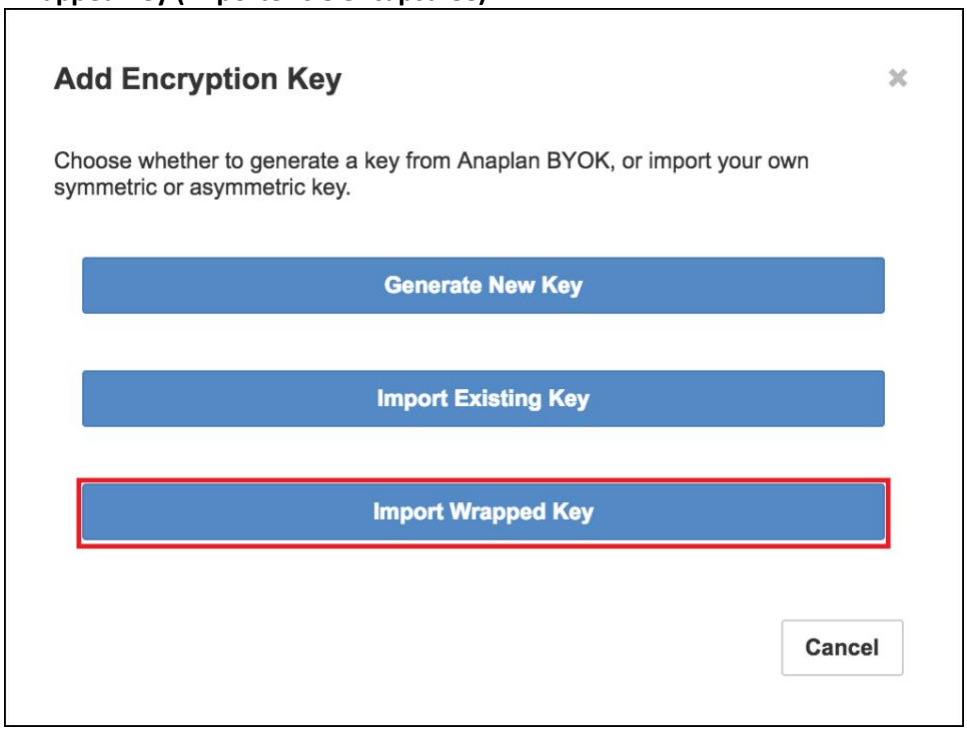
ADMINISTRATEURS DU CHIFFREMENT UNIQUEMENT

Importez la clé encapsulée.

1. Dans l'encadré Anaplan Administration, sous BYOK, sélectionnez **Encryption Keys (Clés de chiffrement).**
2. Cliquez sur **Add Key (Ajouter une clé)**.

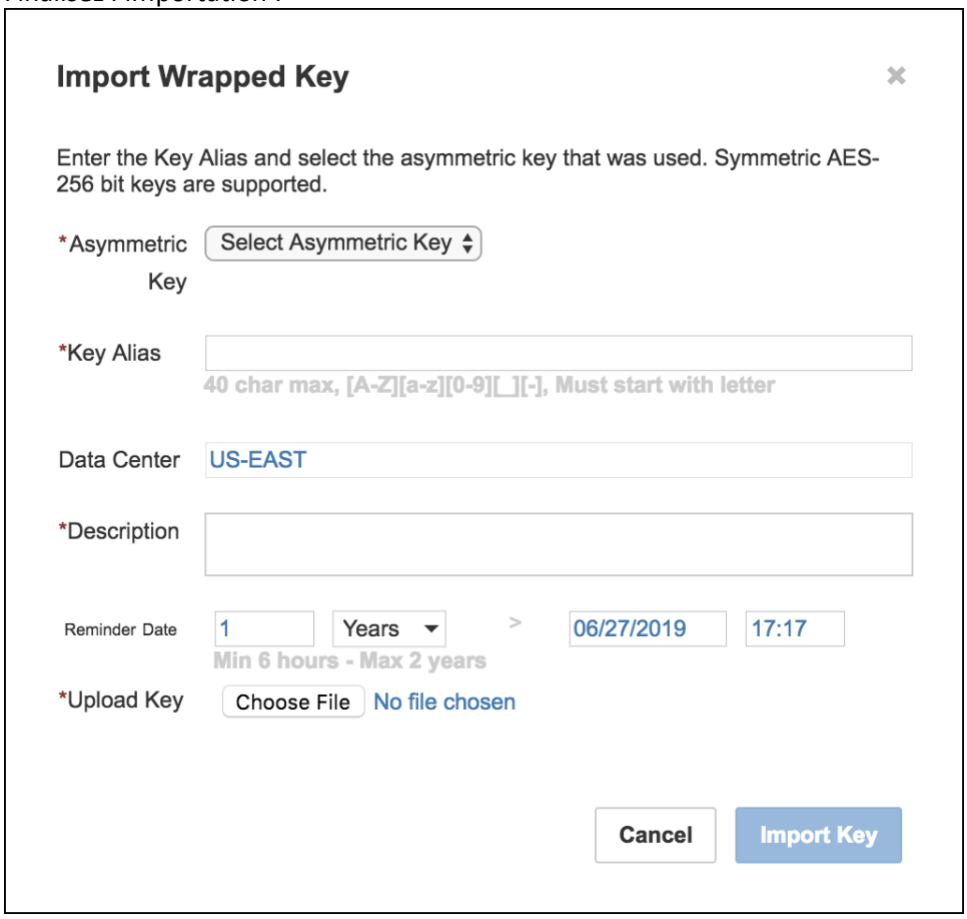
 © Anaplan 2018

3. Dans la boîte de dialogue Add Encryption Key (Ajouter une clé de chiffrement), cliquez sur **Import Wrapped Key (Importer clé encapsulée)**.



 © Anaplan 2018

4. Finalisez l'importation :



- Sélectionnez la clé asymétrique utilisée pour encapsuler la clé symétrique.
- Affectez un alias à la clé symétrique dans le champ Key Alias.
- Définissez la date de rappel dans le champ Reminder Date. La valeur par défaut correspond à 1 an.
- Téléchargez la clé encapsulée.

 © Anaplan 2018

Suppression des clés de chiffrement

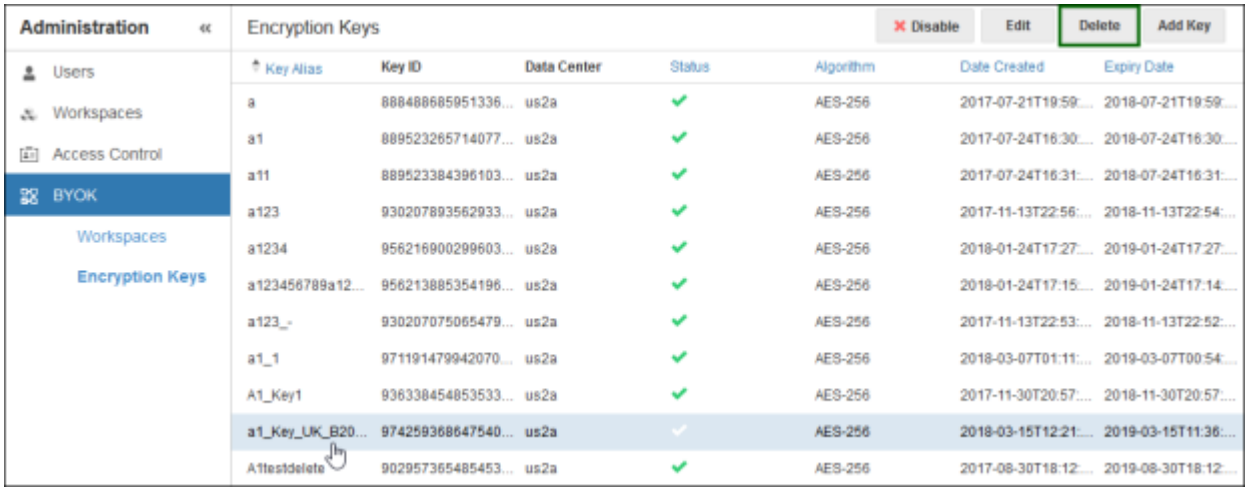
En tant qu'administrateur du chiffrement (Encryption Admin), vous pouvez supprimer une clé symétrique pour l'effacer de Bring Your Own Key (BYOK) en raison d'un manque de confiance dans la clé ou parce qu'elle est devenue superflue.

- *Il est impossible de supprimer une clé en cours d'utilisation. Si la clé est utilisée dans un espace de travail actif, vous devez déchiffrer celui-ci ou réaffecter la clé avant de la supprimer.*

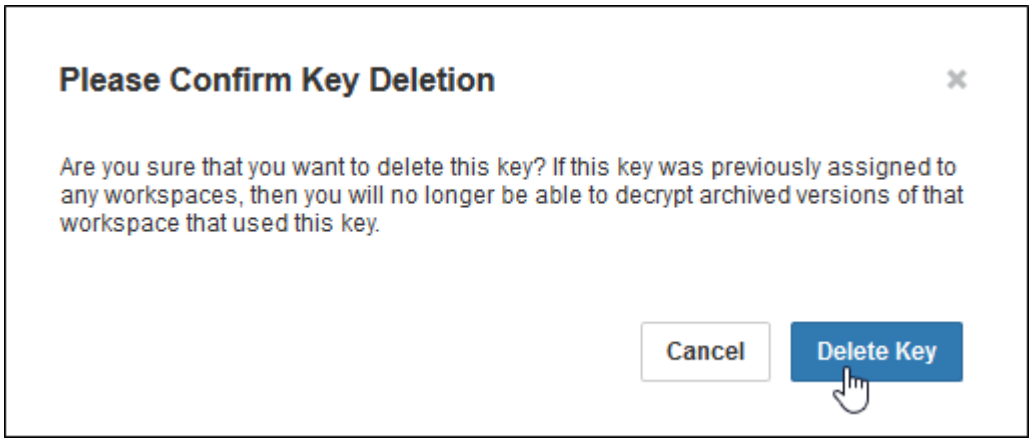
⚠ Si la clé à supprimer avait été précédemment affectée à un espace de travail, vous ne pourrez plus l'utiliser pour déchiffrer les versions archivées de cet espace de travail.

Pour supprimer une clé de chiffrement:

1. Dans l'encadré Anaplan Administration, sous BYOK, sélectionnez **Encryption Keys** (Clés de chiffrement).
2. Sélectionnez la clé de chiffrement à supprimer.
3. Cliquez sur **Delete** (Supprimer).



4. Pour confirmer l'action, cliquez sur **Delete Key** (Supprimer la clé).



 © Anaplan 2018

Désactivation d'une clé de chiffrement

ADMINISTRATEURS DU CHIFFREMENT UNIQUEMENT

Vous pouvez désactiver les clés de chiffrement qui ne sont actuellement pas affectées à un espace de travail. Pour arrêter l'utilisation d'une clé de chiffrement, vous pouvez la désaffecter de chaque espace de travail auquel elle est affectée et la désactiver.

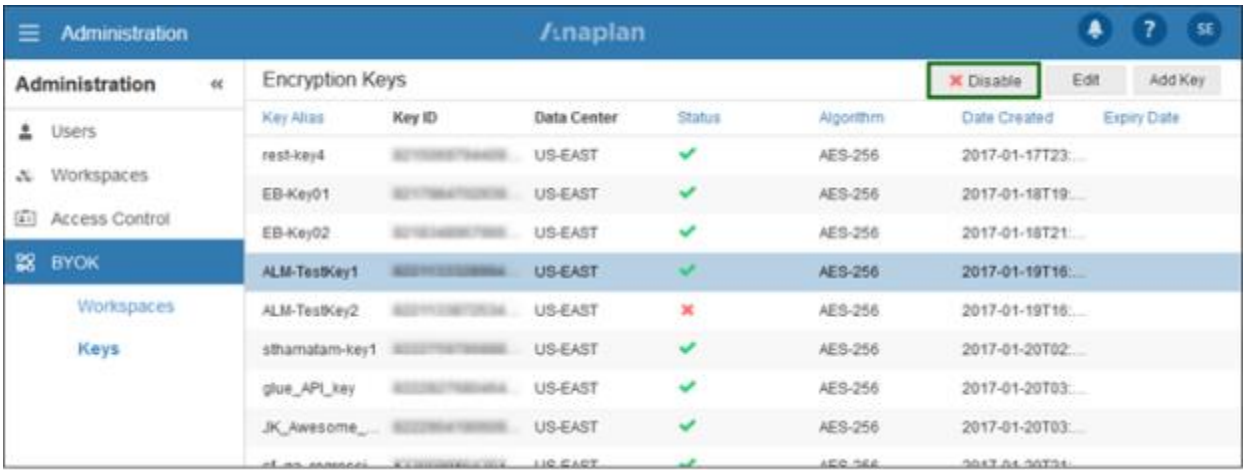
Lorsque vous désactivez une clé de chiffrement :

- La clé est libellée désactivée dans la colonne Status (État) sur la page Encryption Keys (Clés de chiffrement).
- La clé est supprimée des clés disponibles dans la liste déroulante Key (Clé) sur la page Encrypted Workspaces (Espaces de travail chiffrés).
- Les espaces de travail chiffrés à l'aide de cette clé, ainsi que les versions de sauvegarde correspondantes, restent chiffrés.

Pour désactiver une clé de chiffrement :

1. Désaffectez la clé à désactiver dans chaque espace de travail à laquelle elle a été affectée. Voir Désaffectation de la clé de chiffrement d'un espace de travail.
2. Dans l'encadré Administration, sous BYOK, sélectionnez **Keys** (Clés).
3. Sélectionnez la clé active à désactiver.
4. Cliquez sur **Disable** (Désactiver).

La présence d'une croix rouge dans la colonne Status (État) indique que la clé est désactivée.



 © Anaplan 2018

Activation d'une clé de chiffrement

ADMINISTRATEURS DU CHIFFREMENT UNIQUEMENT

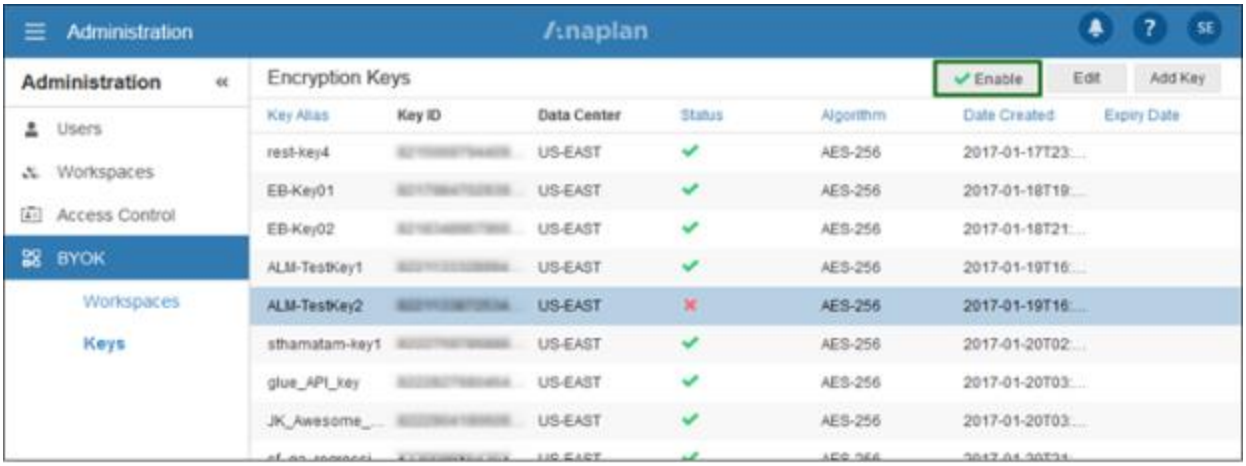
Vous pouvez activer une clé de chiffrement désactivée ou périmée. Lorsque vous activez une clé de chiffrement :

- La clé est libellée activée dans la colonne Status (État) sur la page Encryption Keys (Clés de chiffrement).
- La clé est ajoutée aux clés disponibles dans la liste déroulante Key (Clé) sur la page Encrypted Workspaces (Espaces de travail chiffrés).
- La date de rappel (Reminder Date) n'est pas modifiée.

Pour activer une clé de chiffrement :

1. Dans l'encadré Administration, sous BYOK, sélectionnez **Keys** (Clés).
2. Sélectionnez la clé désactivée à activer.
3. Cliquez sur **Enable** (Activer).

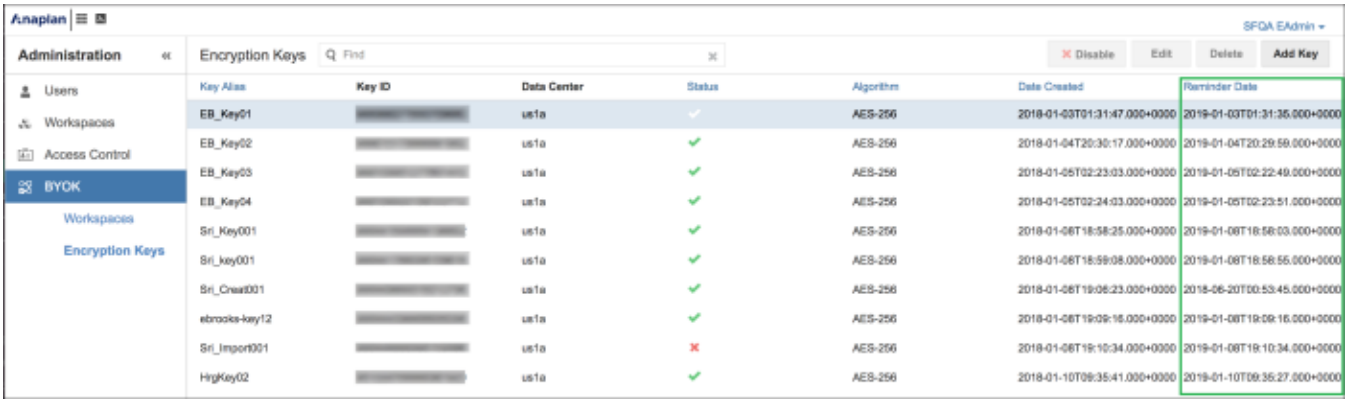
La présence d'une coche verte dans la colonne Status (État) indique que la clé est activée.



 © Anaplan 2018

Rappel associé aux clés

Un rappel est généré pour les clés de chiffrement un an après leur création par défaut. La date que contient la colonne Reminder Date (Date de rappel) vous rappelle de faire tourner chaque clé de chiffrement.



Lorsqu'il est temps de faire tourner une clé de chiffrement :

- La clé est libellée désactivée dans la colonne Status (État) sur la page Encryption Keys (Clés de chiffrement).
- La clé est supprimée des clés disponibles dans la liste déroulante Key (Clé) sur la page Encrypted Workspaces (Espaces de travail chiffrés).
- Les espaces de travail chiffrés à l'aide de cette clé, ainsi que les versions de sauvegarde correspondantes, restent chiffrés.
- Vous pouvez activer la clé. Voir Activation d'une clé de chiffrement.

Modification de la date de rappel d'une clé

ADMINISTRATEURS DU CHIFFREMENT UNIQUEMENT

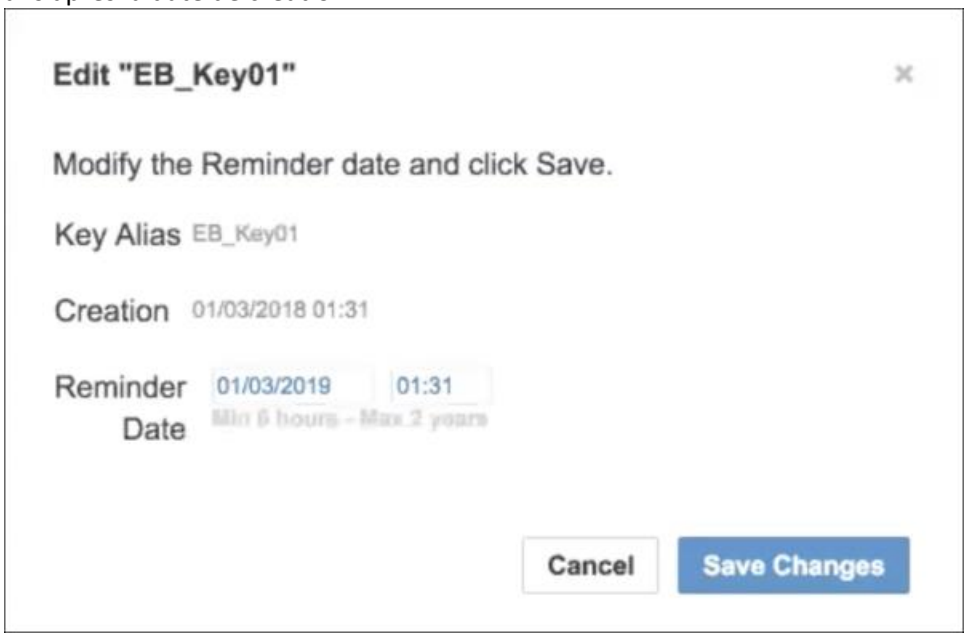
Le rappel associé à une clé de chiffrement est généré 365 jours par défaut après sa date de création. Vous pouvez toutefois modifier la date de rappel d'une clé de chiffrement qui n'a pas encore besoin de tourner. Entrez une date comprise entre six heures et deux ans après la date de création.

Pour modifier la date de rappel d'une clé de chiffrement, procédez comme suit :

1. Dans l'encadré Administration, sous BYOK, sélectionnez **Keys** (Clés).
2. Sélectionnez la clé dont vous voulez modifier la date de rappel.
3. Cliquez sur **Edit** (Modifier).

 © Anaplan 2018

4. Cliquez dans le champ Reminder Date (Date de rappel) et sélectionnez une date qui ne dépasse pas deux ans après la date de création.



5. Cliquez sur **Save Changes** (Enregistrer les modifications).

© Anaplan 2018

Chiffrement d'un espace de travail à l'aide de l'une de vos clés de chiffrement

ADMINISTRATEURS DU CHIFFREMENT UNIQUEMENT

Vous pouvez vous approprier et gérer le chiffrement des données de votre locataire en affectant des clés de chiffrement à des espaces de travail donnés. Lorsqu'une clé a été affectée à un espace de travail, elle permet de chiffrer chaque modèle (ou fichier) de l'espace de travail si les données sont au repos.

⚠ **Avertissement :** réfléchissez aux tenants et aboutissants du chiffrement d'un espace de travail. Seul un administrateur du chiffrement est en mesure de désaffecter une clé d'un espace de travail chiffré par BYOK et de réactiver le chiffrement par clé principale défini par défaut. Aucun mécanisme ne permet au personnel Anaplan d'accéder à vos clés. Par conséquent, le personnel Anaplan n'est pas en mesure de chiffrer ou de déchiffrer vos espaces de travail à votre place.

Considérations à prendre en compte lors d'un chiffrement initial

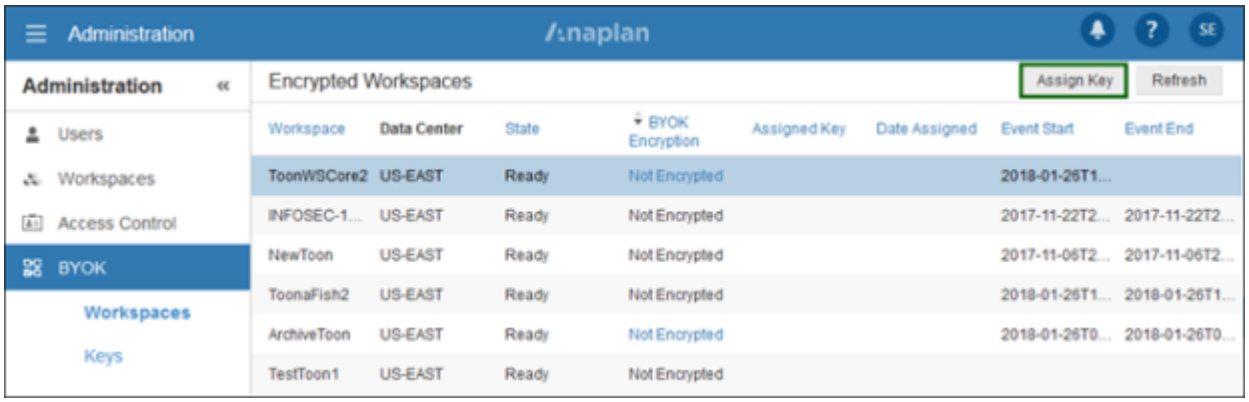
Tenez compte des éléments suivants avant de procéder au chiffrement initial d'un espace de travail à l'aide de l'une de vos clés de chiffrement.

- Le chiffrement ou le déchiffrement d'un espace de travail doit être considéré comme une opération de maintenance qui nécessite une interruption du service.
- Étant donné que la solution BYOK d'Anaplan ne chiffre que les données au repos, il est impossible de chiffrer ou de déchiffrer des données si des utilisateurs sont connectés ou s'ils utilisent des modèles intégrés à l'espace de travail à chiffrer.
- Le chiffrement initial d'un espace de travail est parfois long, en particulier s'il est de taille élevée.
- Lorsque le chiffrement d'un espace de travail est en cours d'exécution, les modèles qu'il contient ne sont pas affichés sur l'écran Tiles (Mosaïques). Ils sont en effet hors ligne à titre temporaire.
- Dans le cadre d'une utilisation standard, les utilisateurs peuvent accéder normalement sur l'écran Tiles (Mosaïques) aux modèles d'un espace de travail chiffré par BYOK.
- Désactivez les intégrations planifiées pendant le chiffrement d'un espace de travail. Les modèles d'un espace de travail ne sont pas disponibles pendant le chiffrement de ce dernier.

Affectation d'une clé à un espace de travail

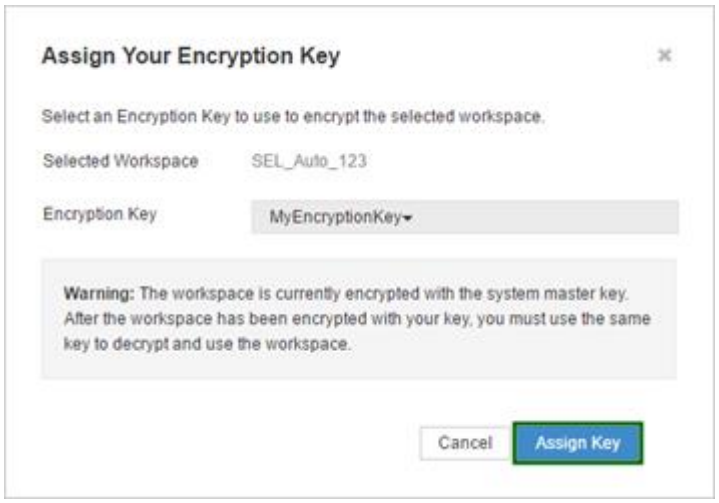
1. Dans l'encadré Anaplan Administration, sous BYOK, sélectionnez **Workspaces** (Espaces de travail).
2. Sélectionnez l'espace de travail auquel vous voulez affecter l'une de vos clés, puis cliquez sur **Assign Key** (Affecter une clé).

 © Anaplan 2018



- Vous pouvez affecter une clé à tout espace de travail dont l'état (State) est Ready (Prêt), dont le statut BYOK est Not Encrypted (Non chiffré) et dont le champ Assigned Key (Clé affectée) est vide.
- Les colonnes Event Start (Début d'événement) et Event End (Fin d'événement) s'affichent lorsqu'un événement de chiffrement d'un espace de travail démarre et prend fin. Un événement de chiffrement démarre lorsque vous affectez une clé de chiffrement. Il prend fin lorsque l'espace de travail est chiffré.
- Cliquez sur Refresh (Actualiser) pour consulter l'état (State) le plus récent de chaque espace de travail.

3. Dans la boîte de dialogue Assign your Encryption Key (Affecter votre clé de chiffrement), procédez comme suit :



4. Sélectionnez la clé de chiffrement à utiliser pour chiffrer l'espace de travail sélectionné.
5. Si vous êtes absolument certain de vouloir chiffrer vos données de modèle à l'aide de votre clé, cliquez sur **Assign Key** (Affecter une clé).

Vous pouvez consulter le déroulement du chiffrement dans BYOK > Workspaces (Espaces de travail), dans la colonne BYOK. Lorsque le statut BYOK est remplacé par Encrypted (Chiffré), l'espace de travail reste chiffré via la clé affectée.

 © Anaplan 2018

Espaces de travail ayant l'état (State) Ready (Prêt)

Dans BYOK > Workspaces (Espaces de travail), la colonne State (État) indique si les espaces de travail sont prêts à être chiffrés avec l'une de vos clés. Seuls les espaces de travail ayant l'état (State) Ready (Prêt) peuvent être chiffrés à l'aide de clés générées ou téléchargées via BYOK. Exemple :

Dans un espace de travail ayant l'état (State) Ready (Prêt) :

- Aucun utilisateur connecté n'accède à un modèle.
- Les modèles sont inactifs depuis un certain temps et ne sont plus actifs en mémoire.

Si votre espace de travail n'a pas l'état (State) Ready (Prêt), contactez l'équipe de support et demandez-lui de décharger l'espace de travail.

 © Anaplan 2018

Déchiffrement d’un espace de travail

ADMINISTRATEURS DU CHIFFREMENT UNIQUEMENT

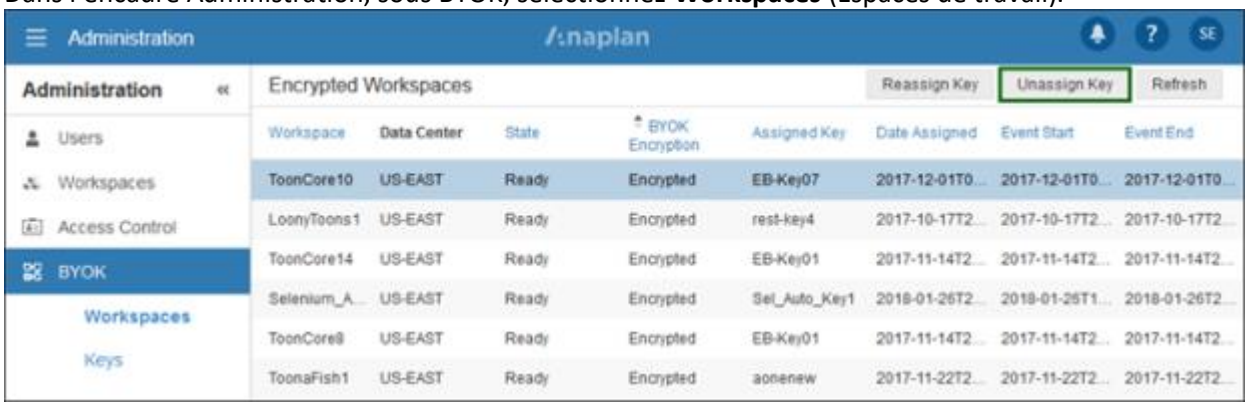
Lorsque vous désaffectez la clé de chiffrement d'un espace de travail, celui-ci est immédiatement chiffré par la clé principale système. Il peut s'avérer nécessaire de désaffecter une clé dans plusieurs cas de figure :

- Votre politique de rotation des clés stipule que vous devez faire tourner les clés entre les espaces de travail chiffrés via BYOK à intervalle fixe.
- Le chiffrement de l'espace de travail à l'aide d'une clé BYOK n'est plus nécessaire.

Toutes les données de modèle d'un espace de travail restent chiffrées pendant le processus de désaffectation des clés.

Pour désaffecter la clé d'un espace de travail, procédez comme suit :

1. Dans l’encadré Administration, sous BYOK, sélectionnez **Workspaces** (Espaces de travail).



2. Sélectionnez un espace de travail dont le statut BYOK est Encrypted (Chiffré).
3. Cliquez sur **Unassign Key** (Désaffecter la clé).
4. Dans la boîte de dialogue Unassign Your Encryption Key (Désaffecter votre clé de chiffrement), cliquez sur **Unassign Key** (Désaffecter la clé) si vous êtes absolument certain de vouloir désactiver le chiffrement de l'espace de travail à l'aide de votre clé.

 © Anaplan 2018

Vous pouvez consulter le déroulement du déchiffrement dans BYOK > Workspaces (Espaces de travail), dans la colonne BYOK. Une fois le déchiffrement terminé, le statut est remplacé par Not Encrypted (Non chiffré). L'espace de travail est maintenant chiffré à l'aide de la clé principale système.

© Anaplan 2018

Rotation des clés

Une politique de rotation des clés détermine la fréquence à laquelle une entreprise doit faire tourner les clés entre différents jeux de fichiers chiffrés au sein d'une application.

Vous pouvez faire tourner les clés à fréquence régulière pour vous conformer à votre politique d'entreprise et pour réduire le volume de contenus chiffrés à l'aide d'une clé unique. Seuls les administrateurs du chiffrement sont autorisés à activer la rotation des clés.

En tant qu'administrateur du chiffrement, vous pouvez faire tourner la clé affectée à un espace de travail dont le statut BYOK est Encrypted (Chiffré) à l'aide du bouton **Reassign Key** (Réaffecter la clé).

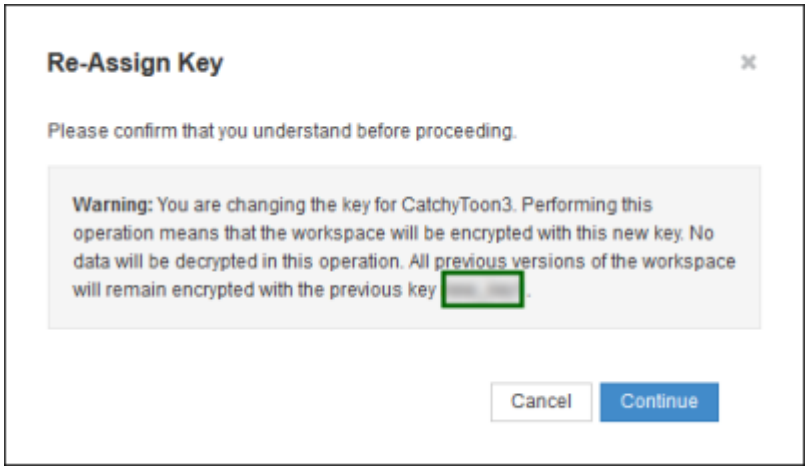
Remarque : *pour que vous puissiez faire tourner une clé, l'espace de travail doit avoir l'état (State) « Ready » (Prêt). Voir Espaces de travail ayant l'état (State) Ready (Prêt).*

Avertissement : lorsque vous réaffectez la clé de chiffrement d'un espace de travail, celui-ci n'est pas déchiffré. La réaffectation est effectuée hors ligne et cet espace de travail n'est pas disponible tant que l'opération n'est pas terminée.

Pour faire tourner la clé d'un espace de travail chiffré, procédez comme suit :

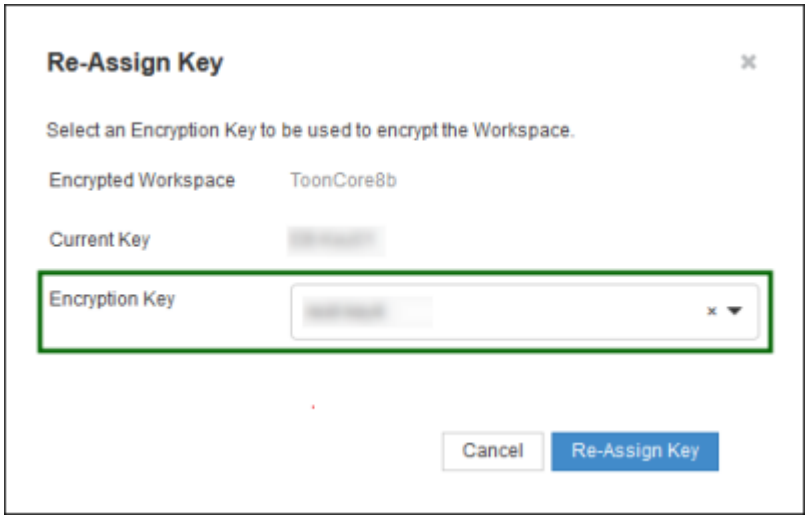
1. Dans l'encadré Anaplan Administration, sous BYOK, sélectionnez **Workspaces** (Espaces de travail).
2. Sélectionnez l'espace de travail pour lequel vous voulez faire tourner la clé de chiffrement.
3. Cliquez sur **Re-Assign Key** (Réaffecter la clé).

   Remarque : toutes les versions antérieures de cet espace de travail restent chiffrées à l'aide de la clé précédente. Nous vous recommandons de prendre note de cette clé à titre de référence.



4. Cliquez sur **Continue** (Continuer).
5. Sélectionnez la **clé de chiffrement** à utiliser.

© Anaplan 2018



6. Cliquez sur **Re-Assign Key** (Réaffecter la clé).

   Le statut BYOK est remplacé par *In Progress* (En cours). Une fois l'opération terminée, le statut BYOK est *Encrypted* (Chiffré).

7. Cliquez sur **Refresh** (Actualiser) pour consulter l'état (State) le plus récent de chaque espace de travail.

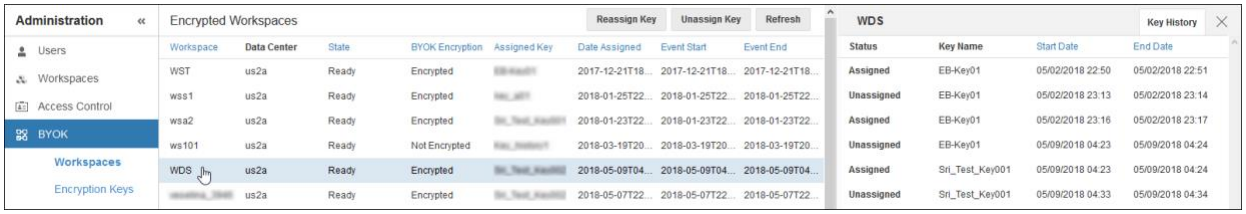
© Anaplan 2018

Affichage de l'historique des clés

Lorsque vous avez fait tourner vos clés, vous pouvez afficher les clés utilisées pour chiffrer vos espaces de travail dans BYOK. Ces informations sont également disponibles dans les journaux d'audit.

Pour consulter l'historique des clés d'un espace de travail dans BYOK, procédez comme suit :

1. Dans l'encadré Administration, sous BYOK, sélectionnez **Workspaces** (Espaces de travail).
2. Sélectionnez l'espace de travail pour lequel vous voulez afficher l'historique des clés de chiffrement.



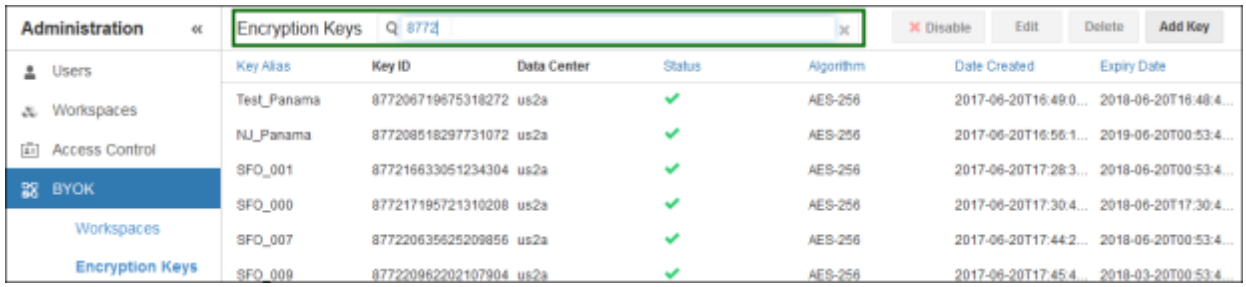
L'onglet **Key History** (Historique des clés) contient l'historique des événements de clés de chiffrement associé à l'espace de travail, à savoir :

- Nom de la clé
- Statut de chaque événement de clé de chiffrement, soit :
  - Assigned (Assigné)
  - Unassigned (Non assigné)
  - Assignment Failed (Affectation a échoué)
  - Unassignment Failed (Annulation d'affectation a échoué)
- Dates de début et de fin de l'événement

 © Anaplan 2018

Recherche d’une clé de chiffrement

La page Encryption Keys (Clés de chiffrement) de Bring Your Own Key (BYOK) vous permet de filtrer la liste des clés de chiffrement à partir de leur alias (Key Alias) ou de leur ID (Key ID). Pour filtrer la liste, entrez les premiers caractères de l’alias ou de l’ID dans la zone Find (Rechercher).



 © Anaplan 2018

Notifications relatives aux événements de chiffrement

Lorsque certains événements de chiffrement sont exécutés dans BYOK, l'administrateur du chiffrement reçoit des notifications par le biais de l'application Anaplan Notifications et par e-mail.

Les événements suivants génèrent des notifications :

- Le chiffrement de l'espace de travail est terminé.
- Le déchiffrement de l'espace de travail est terminé.
- Le chiffrement a échoué.
- Une clé a été supprimée.
- Une clé a été désactivée.

© Anaplan 2018

Quelles sont les données chiffrées par BYOK ?

Chaque modèle Anaplan, y compris les modèles figurant dans les espaces de travail chiffrés via BYOK, se compose d'informations structurelles et de données de production.

- Les informations structurelles comportent les paramètres de configuration d'un modèle et des listes (à l'exception des listes de production indiquées). Pour capturer le dernier état en date assigné aux informations structurelles d'un modèle, ajoutez une balise de révision.
- Les données de production comportent les valeurs de cellules, les utilisateurs, les états des flux de travail et le contenu des listes de production indiquées.

Découvrez les objets d'un modèle assimilés à des informations structurelles dans Structural Information Reference (https://community.anaplan.com/anapedia/model-building/alm/model-data/structural-information-reference).

Lorsque vous chiffrez un espace de travail avec votre propre clé de chiffrement, toutes les données de production des modèles que contient l'espace de travail sont chiffrées. Les informations structurelles ne sont en revanche pas chiffrées, puisqu'elles sont stockées en dehors de l'espace de travail parent.

Les données sont chiffrées au repos uniquement, et non lorsqu'elles sont chargées en mémoire. Lorsqu'un modèle est en cours d'utilisation, les données sont déchiffrées et les utilisateurs autorisés les visualisent en clair. Utilisez les rôles et les accès sélectifs pour gérer l'accès aux modèles ou à des listes et regroupements donnés.

© Anaplan 2018

Glossaire des événements et termes de chiffrement

BYOK intègre diverses caractéristiques de sécurité, à savoir :

Caractéristique de sécurité	Description
Garantie de chiffrement	Notre infrastructure de chiffrement comprend un dispositif de gestion des clés certifié FIPS 140-2 de niveau 3. Un module HSM (Hardware Security Module, module de sécurité matériel) intégré fournit les racines de confiance (RoT). Toutes les données sont chiffrées à l'aide de l'algorithme AES (256 bits).
Infrastructure de chiffrement	Vous disposez de notre infrastructure de chiffrement pour gérer le cycle de vie des clés de chiffrement de vos actifs. Elle assure la confidentialité des données et protège le matériel de chiffrement conformément à la norme NIST SP 800-175B. Le cas échéant, vous pouvez télécharger des clés compatibles générées par une application de gestion cryptographique externe.
Chiffrement asymétrique	Également appelé chiffrement par clé publique, le chiffrement asymétrique fait appel à des clés publiques et privées pour chiffrer et déchiffrer les données. La clé exportée d'Anaplan correspond à la clé publique de la paire de clés et l'algorithme utilisé est RSA 2048. Elle sert à encapsuler une clé symétrique.
Chiffrement symétrique	Utilise les mêmes clés de chiffrement pour chiffrer le texte en clair et déchiffrer le texte chiffré.
Chiffrement des données et contrôle des accès	Le chiffrement des données et le contrôle des accès s'appuient sur un pilote de protection des fichiers noyau installé sur le serveur d'applications.
Séparation des tâches	BYOK permet de mettre en œuvre une stratégie robuste de séparation des tâches. La gestion des clés est l'unique responsabilité de l'administrateur du chiffrement et est strictement séparée des autres rôles administratifs de niveaux locataire et espace de travail. BYOK interdit à tout administrateur unique de contrôler l'intégralité des activités de protection des données.
Gestion des clés et chiffrement sous le contrôle du client	Vous contrôlez vos clés et le cycle de vie associé directement dans Anaplan Administration (https://community.anaplan.com/anapedia/tenant-administration). Ni le personnel Anaplan, ni les administrateurs qui ne sont pas chargés du chiffrement au sein de votre entreprise n'ont accès à vos clés ou à vos données de modèle chiffrées.

© Anaplan 2018

Caractéristique de sécurité	Description
Chiffrement transparent	Bien qu'il protège l'ensemble des données d'un modèle chiffré, le chiffrement des données est invisible du point de vue de l'utilisateur final, d'où une réduction de la complexité et du coût des opérations.
Conformité aux impératifs géo-juridiques	BYOK vous permet de stocker vos clés et vos données chiffrées conformément aux impératifs géo-juridiques qui vous incombent (sous couvert d'approbation).
Rapports de conformité	La génération de rapports de conformité fournit des informations concernant le chiffrement, la gestion des clés et les actions associées à la politique d'accès, par utilisateur et date/heure. Le journal consigne chaque utilisateur et processus qui tente d'accéder aux données de protection du chiffrement, que l'opération aboutisse ou non.
Clé encapsulée	Clé symétrique AES-256 encapsulée dans une clé asymétrique générée par Anaplan.

© Anaplan 2018

Enable Support Access (Activer l'accès support)

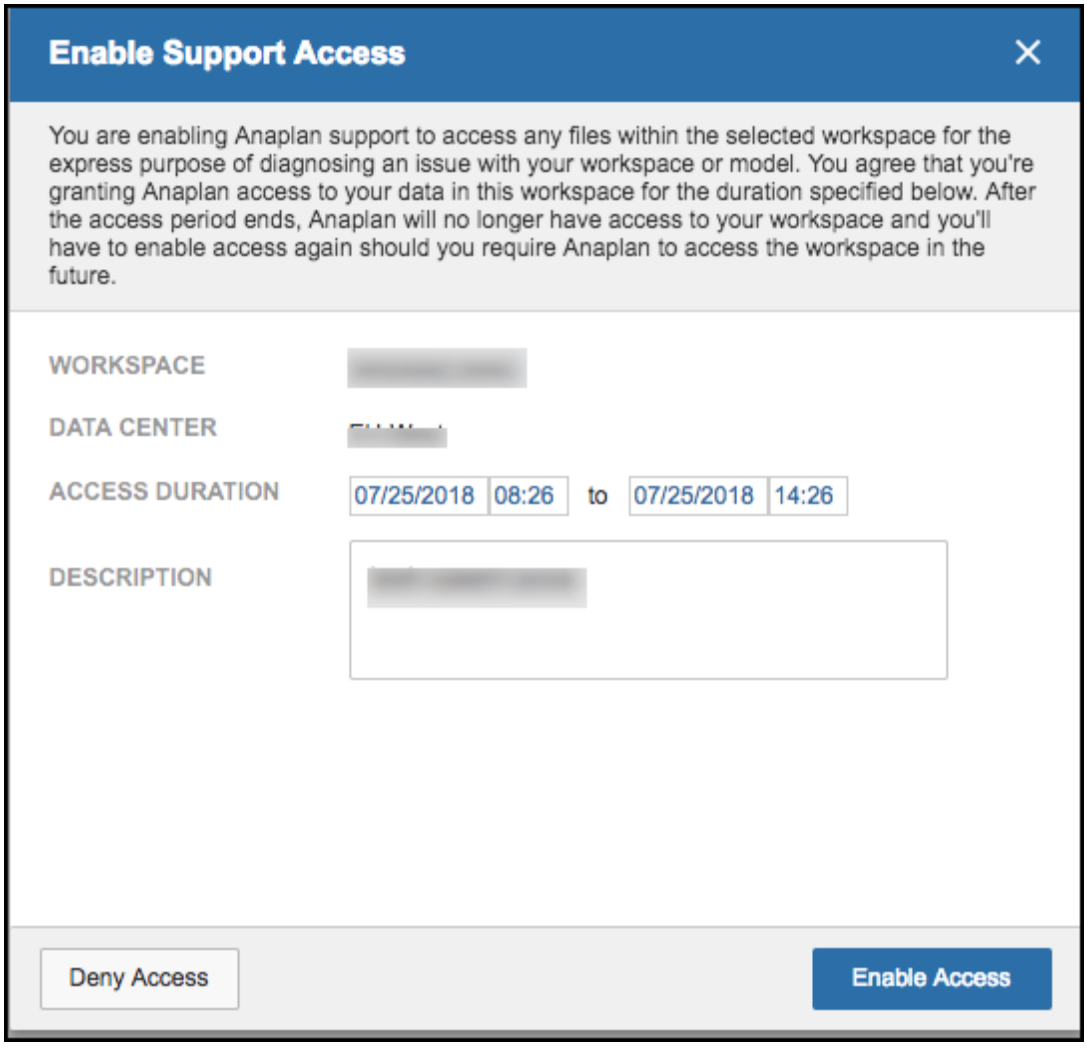
ADMINISTRATEUR DU CHIFFREMENT UNIQUEMENT

Si l'équipe de support a demandé à accéder à votre espace de travail, vous devez activer l'accès support pour autoriser la procédure. En autorisant l'équipe de support à accéder à votre espace de travail BYOK, vous acceptez qu'elle accède aux modèles de cet espace de travail, aux données qu'ils contiennent et à l'historique de modification des modèles.

Activation de l'accès à partir d'une demande de l'équipe de support

Si l'équipe de support Anaplan a demandé à accéder à un espace de travail, les notifications de demande en attente sont affichées lorsque vous sélectionnez l'interface Workspaces (Espaces de travail).

1. Accédez à **Administration > BYOK > Workspaces (Espaces de travail)**.
2. Examinez la demande d'accès affichée dans la boîte de dialogue Enable Support Access (Activer l'accès support).



La demande d'accès comprend les données suivantes :

- nom de l'espace de travail,

 © Anaplan 2018

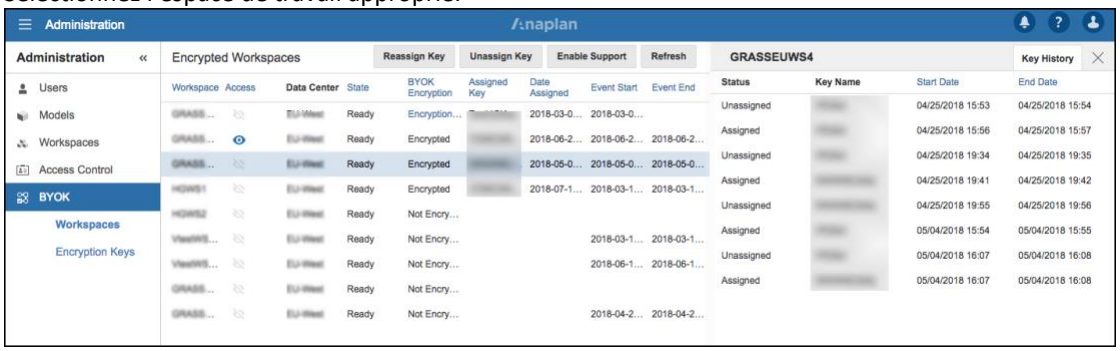
- code du centre de données,
- durée de l’accès,
- motif de la demande d’accès à l’espace de travail par l’équipe de support.

3. Cliquez sur **Enable Access (Activer l’accès)** pour autoriser l’équipe de support Anaplan à accéder à l’espace de travail ou sur **Deny Access (Refuser l’accès)** pour refuser l’autorisation d’accès.

Activation de l’accès sans demande de l’équipe de support

L'administrateur du chiffrement peut autoriser de manière proactive les analystes de l’équipe de support à accéder à votre espace de travail. Procédez comme suit :

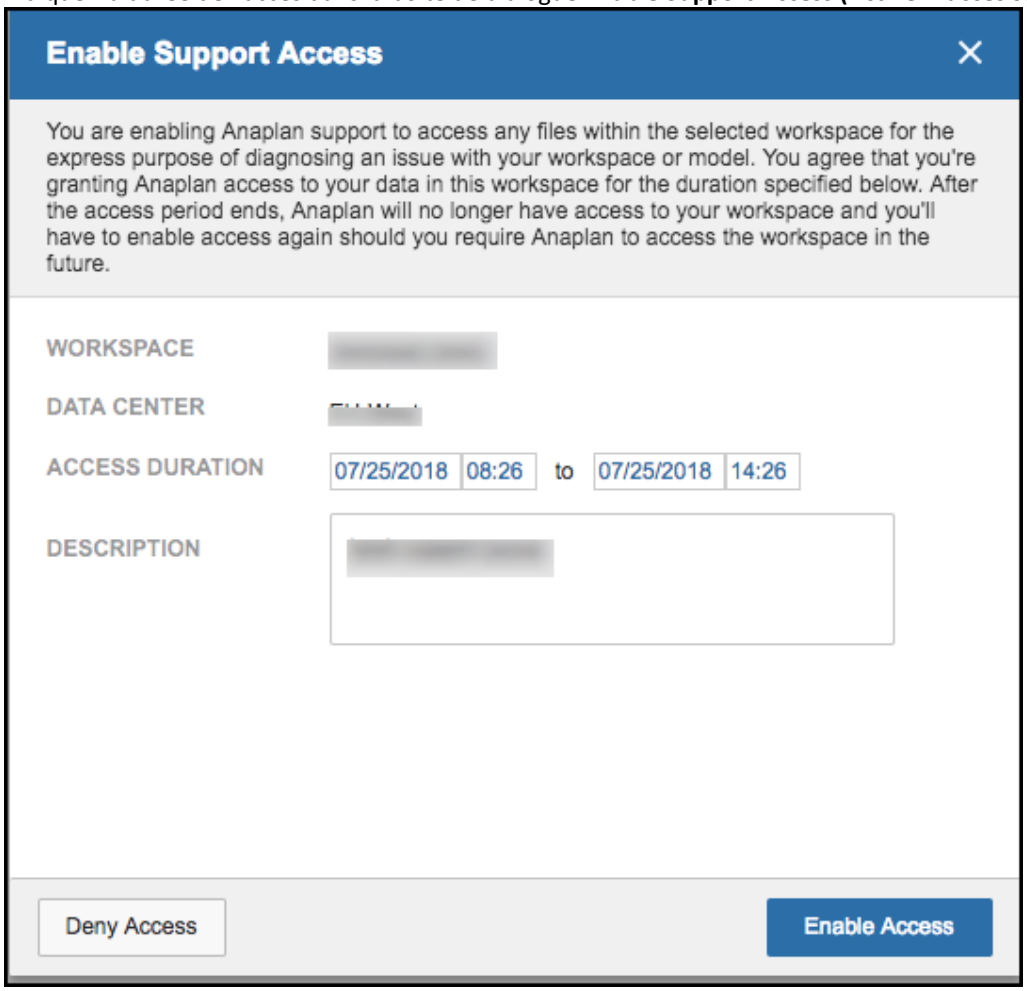
1. Accédez à **Administration > BYOK > Workspaces (Espaces de travail)**.
2. Sélectionnez l’espace de travail approprié.



3. Cliquez sur **Enable Support (Activer l’accès support)**.

 © Anaplan 2018

4. Indiquez la durée de l'accès dans la boîte de dialogue **Enable Support Access (Activer l'accès support)**.

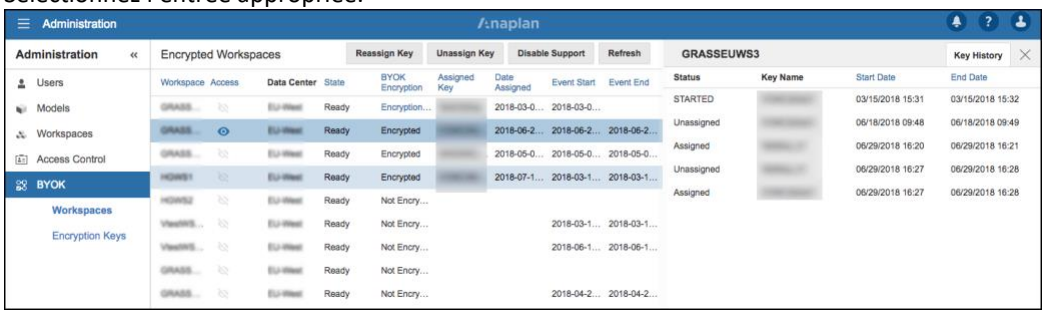


5. Cliquez sur **Enable Access (Activer l'accès)**.

Disable Support Access (Désactiver l'accès support)

Pour interdire aux analystes de l'équipe de support Anaplan d'accéder à votre espace de travail, procédez comme suit :

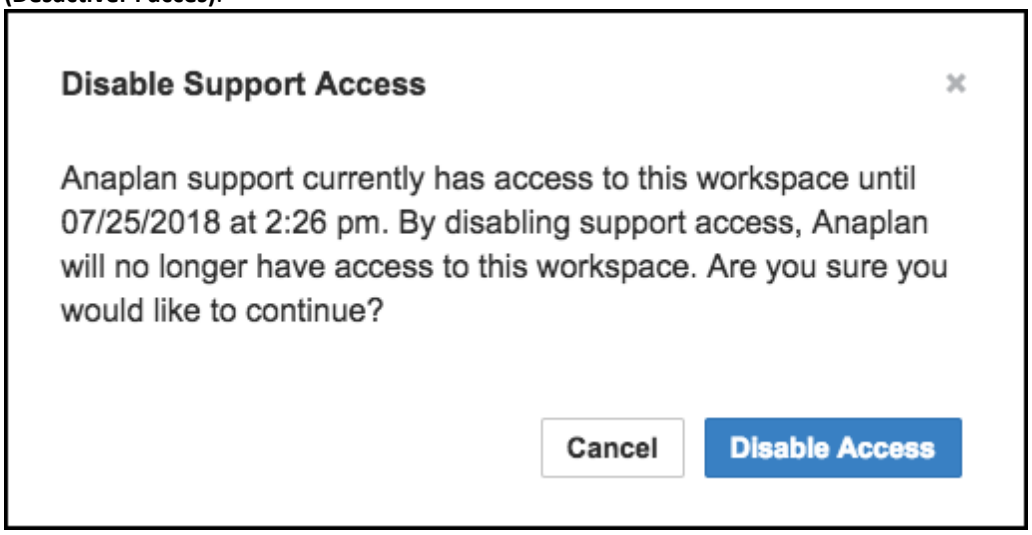
1. Accédez à **Administration > BYOK > Workspaces (Espaces de travail)**.
2. Sélectionnez l'entrée appropriée.



3. Cliquez sur **Disable Support (Désactiver l'accès support)**.

 © Anaplan 2018

4. Dans la boîte de dialogue **Disable Support Access (Désactiver l'accès support)**, cliquez sur **Disable Access (Désactiver l'accès)**.



Affichage de l'accès support

1. Accédez à **Administration > BYOK > Workspaces (Espaces de travail)**.
2. Affichez les entrées.
   - L'icône indique que l'équipe de support Anaplan est autorisée à accéder à l'espace de travail.
   - L'icône indique que l'équipe de support Anaplan n'est pas autorisée à accéder à l'espace de travail.

 © Anaplan 2018

Journaux d’audit

Vous disposez d’Anaplan Audit pour récupérer les journaux d’audit de Bring Your Own Key (BYOK). Vous pouvez consulter les événements d'audit dans l’application Anaplan Administration. Vous pouvez également utiliser l’API Anaplan Audit pour extraire des informations relatives aux événements d'audit. Anaplan Audit fournit les éléments suivants :

- Des journaux de chiffrement (disponibles si votre entreprise utilise BYOK).
- Des journaux d’audit relatifs aux activités des utilisateurs (disponibles si votre entreprise a accès à Anaplan Audit).

© Anaplan 2018

Glossaire des événements de chiffrement

Terme	Définition	
Processus de chiffrement		
add guardpoint with Policy = AuditKey_encrypt_dxformPolicy	L'espace de travail spécifié dans l'attribut Object ID du journal est sur le point d'être chiffré. L'accès à l'espace de travail est temporairement interdit afin qu'aucun élément ne soit ajouté ou supprimé pendant le processus de chiffrement.	Étapes du processus de chiffrement d'un espace de travail
marked guardpoint pending delete with Policy = AuditKey_encrypt_dxformPolicy	L'espace de travail est chiffré.	
delete pending guardpoint with Policy = AuditKey_encrypt_dxformPolicy	La restriction interdisant tout accès pendant le chiffrement est désactivée.	
add guardpoint with Policy = AuditKey_policy	Définition de la politique et du contrôle des accès à l'espace de travail. À partir de maintenant, les fichiers ajoutés à l'espace de travail chiffré sont chiffrés au fur et à mesure des ajouts.	
Processus de déchiffrement		
marked guardpoint pending delete with Policy = AuditKey_policy	L'espace de travail spécifié dans l'attribut Object ID du journal est sur le point d'être déchiffré. La politique permettant d'accéder à l'espace de travail pour déchiffrer en toute sécurité les données est sur le point d'être désactivée.	Étapes du processus de déchiffrement d'un espace de travail
delete pending guardpoint with Policy = AuditKey_policy	L'accès à l'espace de travail est temporairement désactivé afin qu'aucun élément ne soit ajouté ou supprimé pendant le processus de déchiffrement.	
add guardpoint with Policy = AuditKey_decrypt_dx_formPolic	Le déchiffrement de l'espace de travail est activé.	

© Anaplan 2018

Terme	Définition
marked guardpoint pending delete with Policy = AuditKey_decrypt_dxformPolicy	L'espace de travail est déchiffré. Les restrictions d'accès à l'espace de travail sont sur le point d'être désactivées.
delete pending guardpoint with Policy = AuditKey_decrypt_dxformPolicy	L'espace de travail a été déchiffré et l'accès est à nouveau autorisé.
Termes généraux	
Chiffrement asymétrique	Également appelé chiffrement par clé publique, le chiffrement asymétrique fait appel à des clés publiques et privées pour chiffrer et déchiffrer les données. La clé exportée d'Anaplan correspond à la clé publique de la paire de clés et l'algorithme utilisé est RSA 2048. Elle sert à encapsuler une clé symétrique.
Create symmetric key	Un administrateur du chiffrement a créé une clé de chiffrement dans BYOK.
Chiffrement symétrique	Utilise les mêmes clés de chiffrement pour chiffrer le texte en clair et déchiffrer le texte chiffré.
Update key	Un administrateur du chiffrement a mis à jour la date de rappel d'une clé de chiffrement dans BYOK.
Clé encapsulée	Clé symétrique AES-256 encapsulée dans une clé asymétrique générée par Anaplan.

© Anaplan 2018