Analyse des solutions de sécurisation de Microsoft Teams

Par Hugues MEUNIER

Avant-propos

Cet article fait référence aux versions de Microsoft Teams en cours en juillet 2022. Il fait état d'une opinion personnelle.

Les problèmes ?

Microsoft Teams est un outil plébiscité par les utilisateurs depuis 2020. Largement utilisé lors des périodes de confinement, l'outil s'est imposé comme outil de référence pour le travail hybride dans un environnement où le télétravail devient une règle établie.

Néanmoins l'outil pose quelques problèmes au niveau sécurité et le paramétrage par défaut de Microsoft est discutable et doit être complété par des actions de sécurisation que nous allons voir ici.

Les risques identifiés

En terme de risques, certains ont rapport avec Teams lui-même mais d'autres sont plutôt d'ordre général ou lié à l'organisation.

Le premier des risques est lié à la population des invités dans les équipes ou les réunions. Nous avons tous en tête l'intrusion d'un journaliste dans une réunion des ministres européens (réunion supposée confidentielle). Cette réunion n'avait pas été organisée dans Teams mais dans un autre outil mais cela aurait été pareil avec Teams.

Un autre risque est lié à l'organisation et l'utilisation ou le vol de données d'authentification. Les comptes d'administration sont très sensibles ; il faut s'assurer que ceux-ci sont utilisés à bon escient et bien les dissocier des usages de Teams.

Un risque évident de fuite et de vol de données existe dans Teams qui est par essence un outil de collaboration donc de partage d'informations.

Détails sur l'organisation et les mesures à mettre en place dans Azure AD

La première mesure à mettre en place obligatoirement est l'authentification multi-facteur pour les administrateurs. En deuxième, Il convient de s'assurer que ces comptes sont bien réservés à l'administration et qu'ils ne bénéficient d'aucune licence de produit M365 afin de respecter le principe de séparation des droits et rôles.

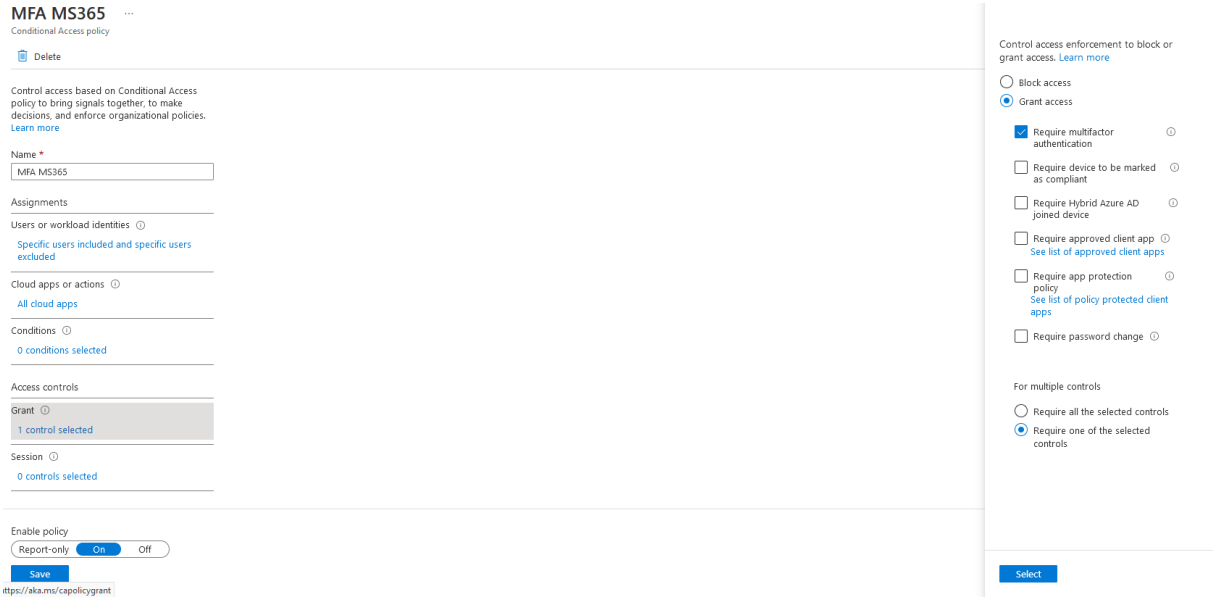
Il faut également dès le début créer les groupes nécessaires au fonctionnalités Teams et mettre en place la gouvernance nécessaire : qui créée ou supprime les équipes ? Comment sont gérer les administrateurs d'équipe ? etc. etc. etc.

Évidemment il faut aussi surveiller, analyser et alerter en fonction des événements.

Mise en place du MFA pour les administrateurs

La mise en place du MFA se fait via la création d'une stratégie d'accès conditionnel :

- https://portal.azure.com
- Azure Active Directory
- Security
- New policy
- Dans « Users or Workload identities », sélectionner « global administrators » ou d'autres rôles que vous souhaitez sécuriser
- Dans « Grant » ajouter un contrôle « Require MFA »

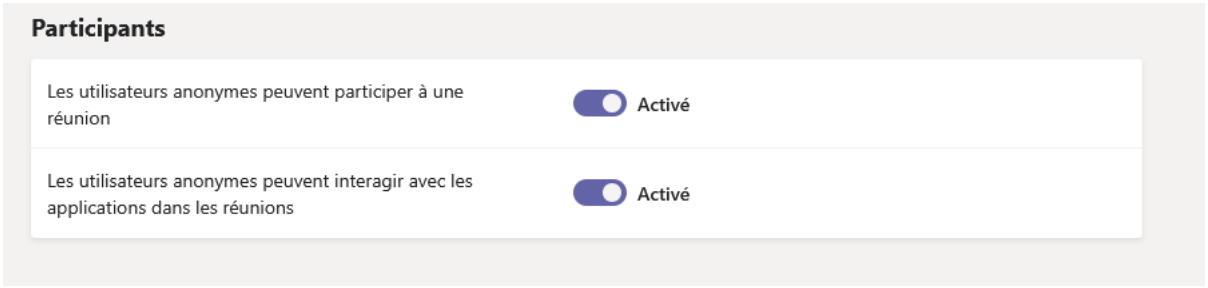


Les stratégies d'accès conditionnels nécessitent Azure AD Premium P1.

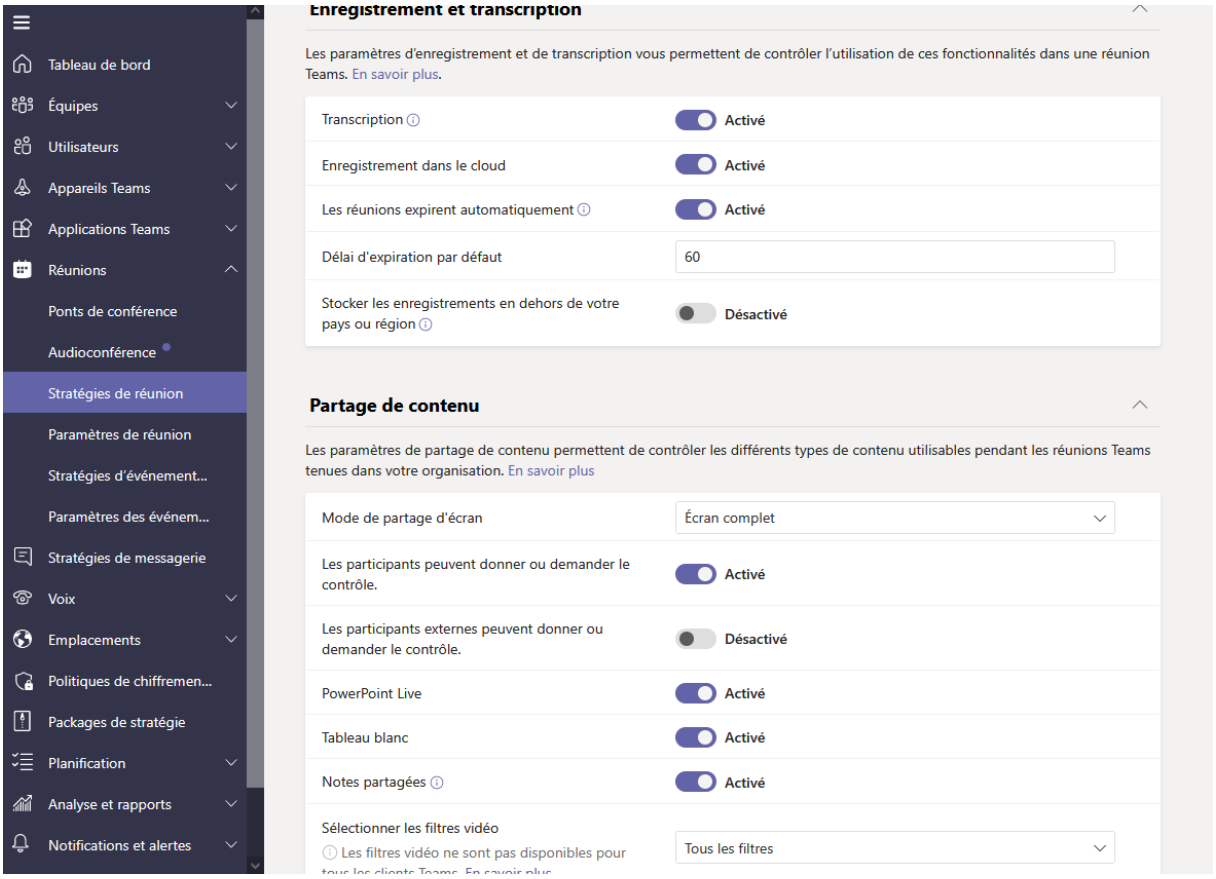
Détails sur les paramètres et stratégies Teams

Les paramètres et stratégies Teams sont accessibles à l'url https://admin.teams.microsoft.com dans Réunions puis Paramètres de réunion et Stratégies de réunion.

Dans paramètres, vous pouvez juste choisir si des utilisateurs anonymes peuvent ou pas participer aux réunions de votre organisation et interagir avec les applications autorisées dans Teams. Par défaut c'est oui pour les deux. Pour limiter les risques, je propose de désactiver le deuxième paramètre.



Dans stratégie de réunion, vous devez modifier certains paramètres dans « Enregistrement et transcription » et dans « Partage de contenu ». Les valeurs par défaut dans la stratégie de base Microsoft sont celles-ci :



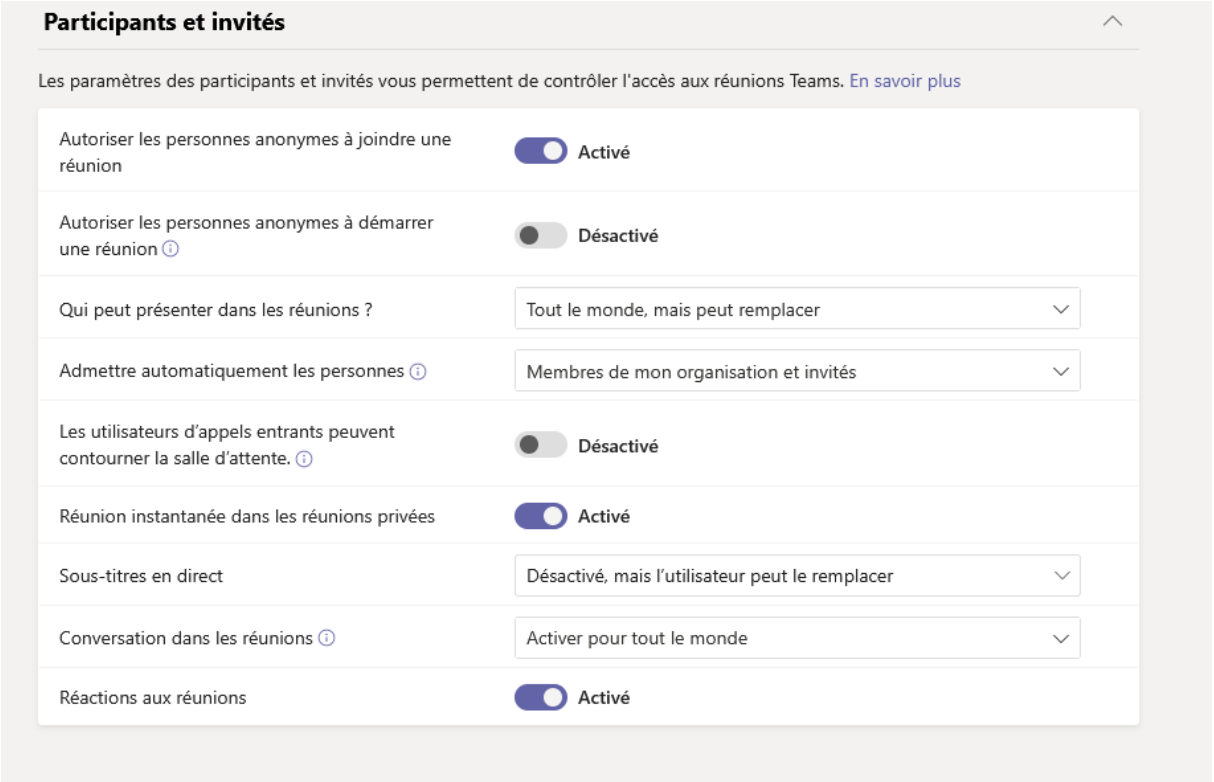
Il faut absolument désactiver le paramètre « les participants externes peuvent donner ou demander le contrôle » pour limiter le risque de prise de contrôle du poste par un invité à une réunion. Ce paramétrage est lié à votre organisation et il restera valable quand l'utilisateur est connecté à votre locataire (votre organisation) même s'il est invité en externe dans une réunion organisée par une autre organisation.

Par contre, si les utilisateurs participent à une réunion en tant qu'invité anonyme alors ce paramètre de stratégie ne s'applique pas et des utilisateurs externes pourront demander le contrôle de l'écran ou de l'application si votre utilisateur est en mode présentation. Pour contrer cette possibilité, il y a la solution du tenant restriction v2.

Mes préconisations sont d'ajuster le délai d'expiration par défaut à une valeur plus faible que 60 jours et de bien désactiver le stockage des enregistrements en dehors de votre pays ou région Azure.

Sélectionner les filtres vidéo doit être modifié pour éviter que les utilisateurs choisissent des images non conformes en fond d'écran de leur vidéo.

Sur la partie « Participants et invités », les valeurs par défaut sont celles-ci :



Mes préconisations sont de :

- Désactivé le paramètre « Autoriser les personnes anonymes à démarrer une réunion »
- Qui peut présenter dans les réunions : mettre « Tous les membres de mon organisation mais les utilisateurs peuvent remplacer »

Détails sur la fonctionnalité en public preview Tenant restriction v2

La fonctionnalité Tenant restriction existe depuis des années sur M365. Elle consistait à intercepter les requêtes https des utilisateurs sur le proxy, à inspecter les trames TLS et à injecter deux valeurs dans les entêtes http :

Pour chaque demande sortante sur login.microsoftonline.com, login.microsoft.com et login.windows.net, insérez deux en-têtes HTTP : *Restrict-Access-To-Tenants* et *Restrict-Access-Context*.

Il est également possible d'empêcher les utilisateurs d'accéder aux outils personnels et aux comptes live personnels en injectant l'entête restrict-msa.

Cette fonctionnalité de tenant restriction a pas mal de défaut ; elle est lourde et complexe et source d'incidents. De plus, elle n'empêche pas les utilisateurs d'accéder en anonyme à des réunions Teams.

La fonctionnalité tenant restriction v2 est en preview publique depuis quelques mois. Elle permet de restreindre la connexion des utilisateurs à des tenants externes (professionnel ou personnel) et surtout d'interdire aux utilisateurs de se connecter en tant qu'anonyme.

La configuration en mode preview n'est pas très simple car il faut injecter une partie de la configuration avec les API REST, une autre avec l'interface d'administration et déployer une GPO ordinateur sur les postes de travail des utilisateurs.

Pour mettre en place le tenant restriction v2, il faut donc injecter la configuration dans graph explorer : https://developer.microsoft.com/en-us/graph/graph-explorer

PATCH https://graph.microsoft.com/beta/policies/crossTenantAccessPolicy/default
Content-Type: application/json

Cet exemple autorise la collaboration B2B sortante mais empêche l'utilisateur de se connecter à des tenants externes et en anonyme.

```
{
   "b2bCollaborationOutbound": {
        "usersAndGroups": {
            "accessType": "allowed",
            "targets": [
                {
                    "target": "AllUsers",
                    "targetType": "user"
                }
            ]
        },
        "applications": {
            "accessType": "allowed",
            "targets": [
                {
                    "target": "Office365",
                    "targetType": "application"
                }
            ]
        }
    },
  "tenantRestrictions":
  {
    "usersAndGroups":
    {
      "accessType": "blocked",
```

```
      "targets": [
        {
          "target": "AllUsers",
          "targetType": "user"
        }
      ]
    },
    "applications":
    {
      "accessType": "blocked",
      "targets": [
        {
          "target": "AllApplications",
          "targetType": "application"
        }
      ]
    }
  }
}
```

Lorsque le PATCH est réalisé, la réponse reçue est http 204.

Ensuite il faut déployer une GPO sur les postes de utilisateurs :

Configuration Ordinateur\Modèles d'administration\Composants Windows\Restrictions de client

Il faut renseigner dans la stratégie :

- ID Azure Active Directory avec l'ID du tenant
- GUID de la stratégie avec l'ID obtenu dans graph explorer. Pour l'obtenir vous pouvez faire un GET de https://graph.microsoft.com/beta/policies/crossTenantAccessPolicy/default

Ne pas oublier de forcer la Maj. des GPO sur le poste gpupdate /force et de rebooter pour la prise en compte.

Le paramétrage du tenant restrictions v2 sera réalisé dans le futur dans la console Azure Active Directory - External identities – Cross-tenant access settings pour la GA. Il n'y a pas de confirmation de la date de mise en GA à ce jour.

Il est possible d'autoriser les utilisateurs à se connecter à certains tenants pour certaines applications. Le tenant restrictions s'applique par défaut sur toutes les applications du poste utilisant l'authentification moderne vers Microsoft (Teams, Outlook, les navigateurs, Onedrive …).

Détails sur les mesures de DLP et de sécurisation des données

La prévention des fuites de données est un vaste sujet et nous n'allons que l'effleurer dans cet article. Qui dit DLP dit classification des données donc la première mesure est la mise en place de cette classification.

Une fois votre classification créée, les utilisateurs devront choisir une étiquette de confidentialité sur chaque document et email qu'ils manipuleront. Ceci constitue un changement important dans les usages et ce changement doit être progressif et accompagné.

Mettre en place la classification avec les étiquettes de confidentialité

La configuration sera réalisée sur la console d'administration de la conformité :

https://compliance.microsoft.com/

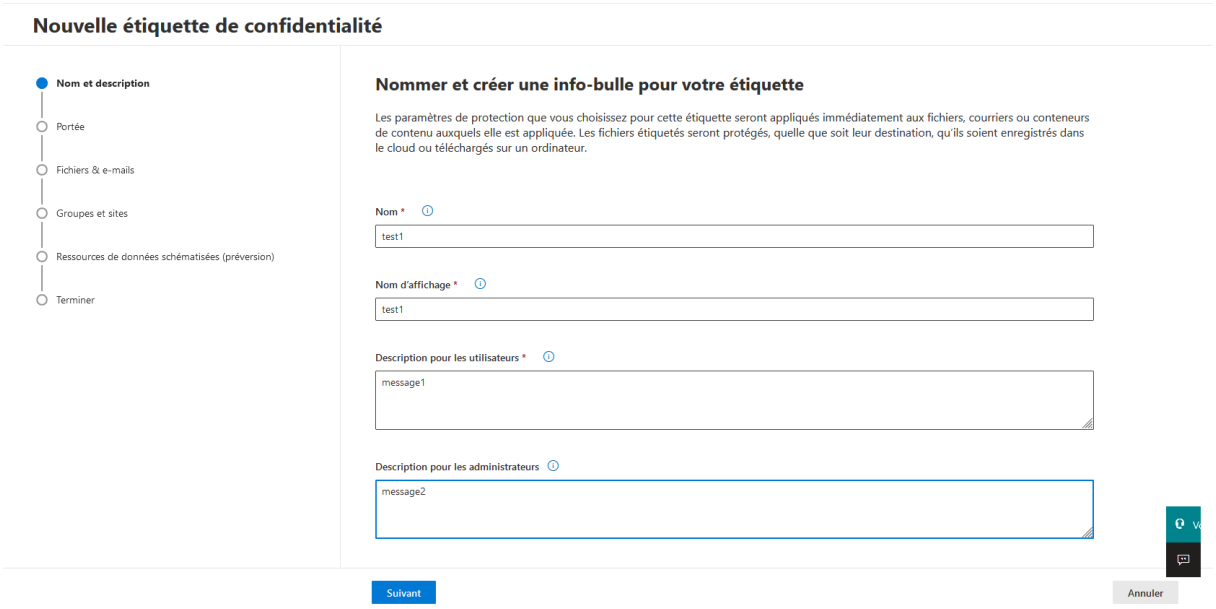
et dans le menu Solutions – Protection des informations puis choisir étiquettes.

Le lien de référence pour ces étiquettes est :

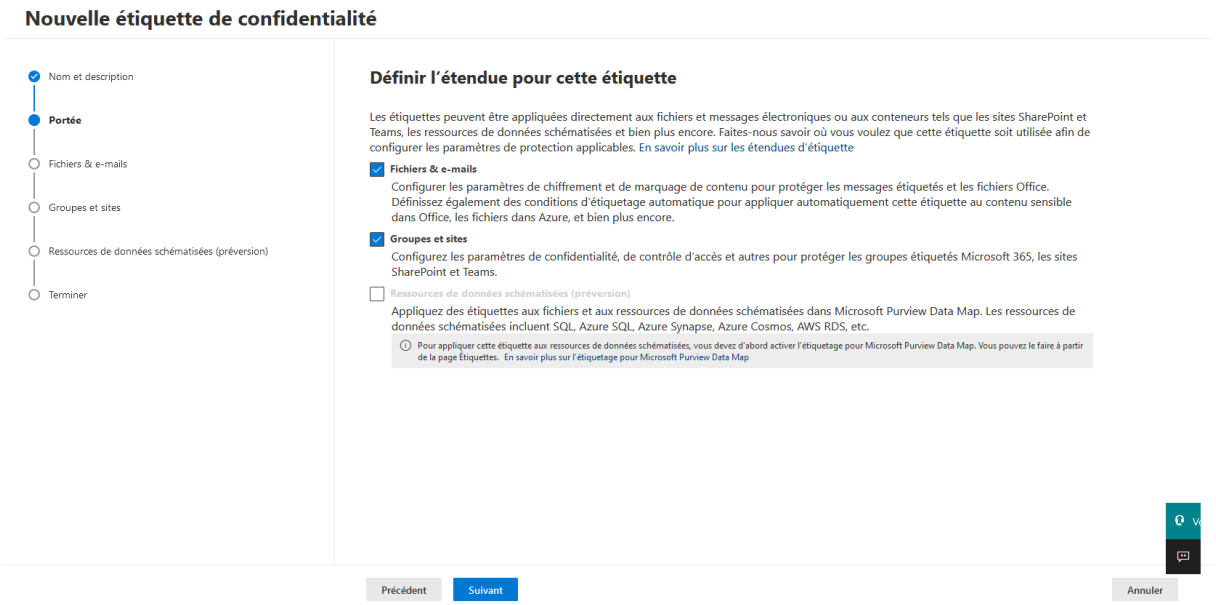
https://docs.microsoft.com/fr-fr/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

La procédure consiste à créer vos niveaux de classification dans l'ordre (très important) de sensibilité (du moins sensible au plus sensible). Par exemple, créer les classifications « publique », « interne » et « confidentiel ».

Remplir le nom et la description :

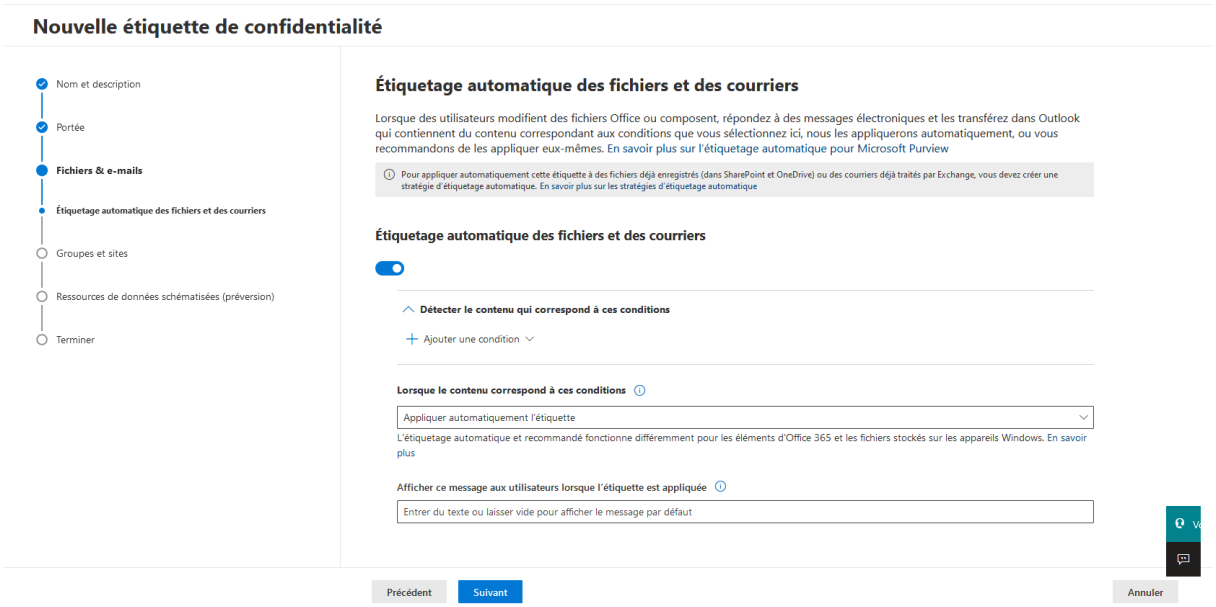


Remplir la portée : Fichiers (Office) et emails (Exchange online), Groupes et sites (Teams, sites Sharepoint) et Ressources de données schématisées (pour les données mais nécessite d'activer Pureview dans le premier écran).

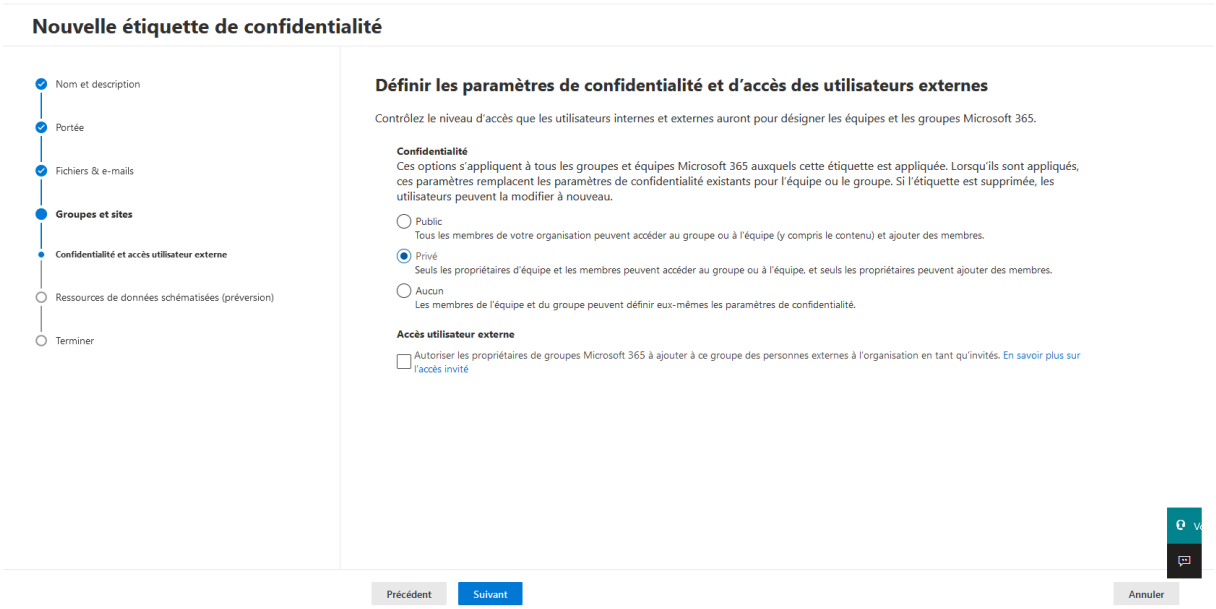


Il est possible de restreindre, chiffrer les accès aux fichiers et email. Il est également possible de marquer le contenu avec un filigrane ou un haut/bas de page.

Il est également possible d'étiqueter automatiquement les fichiers et courriers en fonction de conditions :



Ensuite il faut définir les paramètres de confidentialité des groupes et sites notamment il est possible d'interdire complètement pour une étiquette, les accès utilisateur externe.



Une fois vos classifications créées, il faut créer une stratégie des étiquettes en cliquant sur « Stratégies des étiquettes » et « publier les étiquettes ».

La création de la stratégie consiste à sélectionner les étiquettes à inclure, sélectionner les utilisateurs ou les groupes pour lesquels la stratégie va s'appliquer (attention par défaut c'est tous les utilisateurs et il est fortement conseillé de commencer par un groupe de test avant de généraliser).

Ensuite il faut configurer les paramètres de stratégie notamment on peut obliger les utilisateurs à appliquer une étiquette, appliquer une étiquette par défaut aux documents et emails ou renvoyer les utilisateurs vers un site d'aide à la classification.

Remarque importante pour l'étiquetage automatique

Il existe deux méthode d'étiquetage automatique M365 :

- L'étiquetage côté client qui nécessite d'avoir Office Pro 365 récent ou bien le client d'étiquetage unifié AIP qu'il convient d'installer sur les postes des utilisateurs
- L'étiquetage côté service qui s'applique à l'enregistrement des documents sur M365.

Pour un étiquetage d'un existant, vous n'avez pas le choix il faut mettre en place des stratégies côté service.

Gérer avec DLP les règles de diffusion des documents et emails

Il est important de maîtriser les circuits de diffusion des documents et emails en dehors de l'organisation. Il faut savoir que les documents stockés dans les équipes sont stockés dans le sharepoint online de l'équipe et les documents envoyés dans les discussions le sont dans le onedrive de l'utilisateur.

Il est facile, de base, de partager à l'extérieur des documents car rien ne l'empêche. Vous pouvez appliquer des règles simples pour empêcher le partage d'informations à l'extérieur de votre organisation.

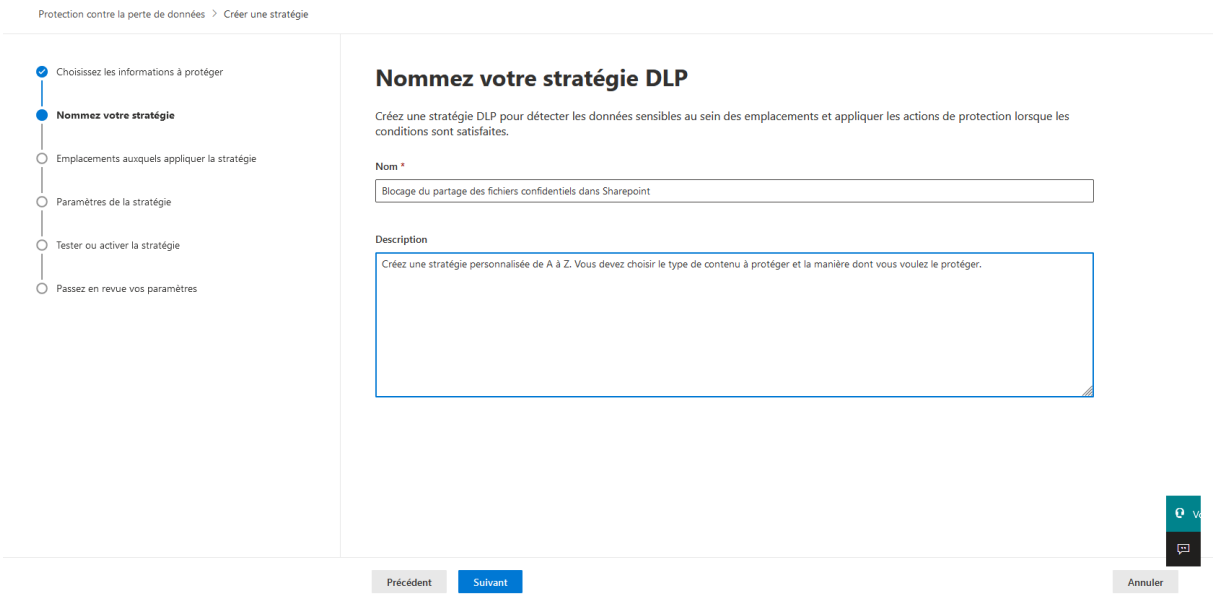
Pour cela, nous allons ouvrir la console de conformité M365 et le menu « Protection contre la perte de données » :

https://compliance.microsoft.com/datalossprevention

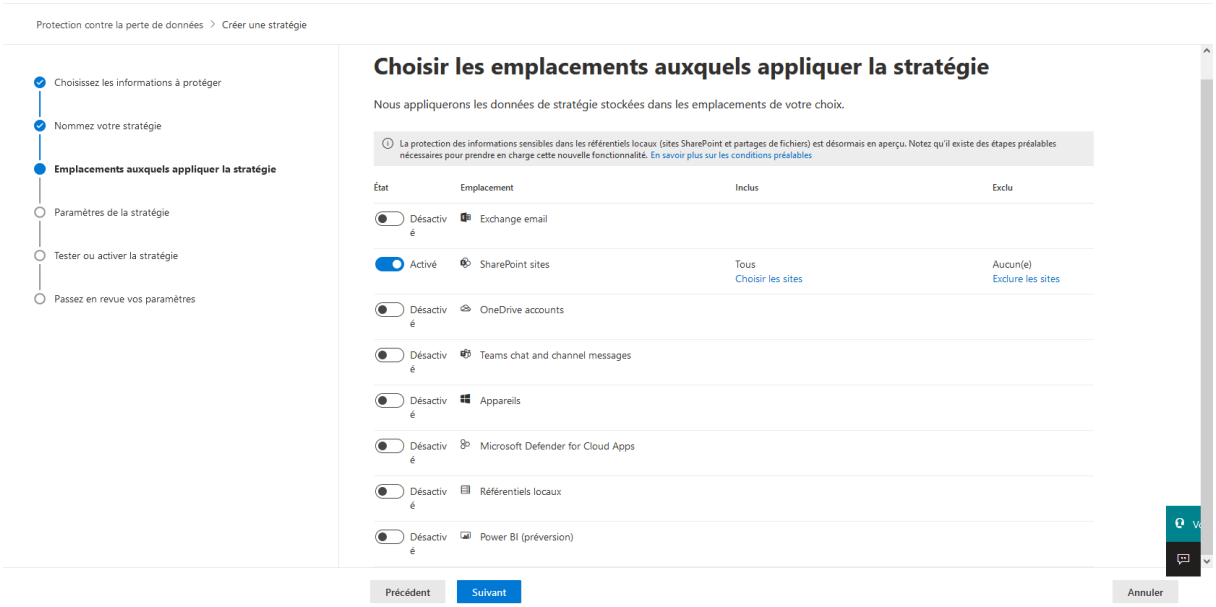
et créer une stratégie pour bloquer le partage en externe des documents ayant une classification confidentielle dans Sharepoint. Vous pouvez appliquer cette stratégie à d'autres outils (Exchange, onedrive, teams) mais il est recommandé de créer une stratégie par outil (pour faire plus facilement le diagnostic en cas de problème).

Dans la console, cliquer sur « Stratégies » puis « créer une stratégie ». Des modèles sont proposés, cliquer sur « Suivant » pour partir d'une stratégie vierge.

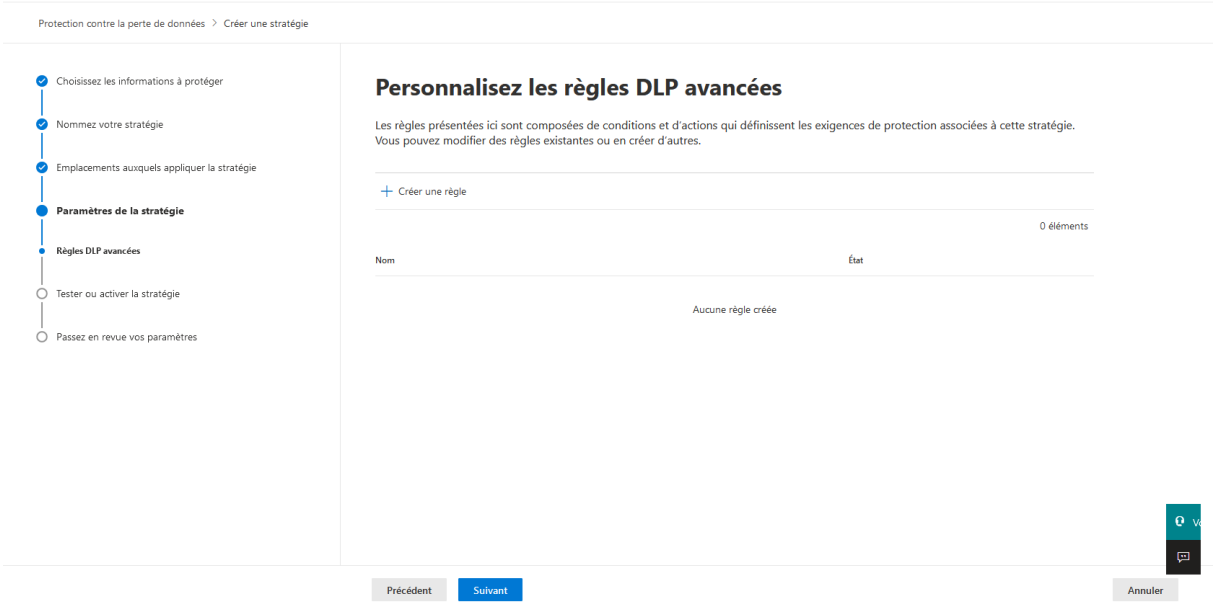
Donner un nom à votre stratégie et remplir le champ « Description » :



Choisissez les emplacements visés par cette stratégie, dans notre exemple ne laisser activé que « Sharepoint sites » puis sélectionner un seul site (dans Choisir les sites) pour restreindre la stratégie et ne pas risquer d'impacter une grande population de vos utilisateurs. Plus tard vous pourrez élargir la portée de la stratégie.



Dans l'écran suivant, nous allons créer les règles DLP qui vont s'appliquer donc cliquer sur « Créer une règle ».



Saisir le Nom et la description de la règle DLP.

Dans conditions, ajouter « Le contenu inclut » - « Étiquettes de confidentialité » puis sélectionner Confidentiel.

Dans conditions, ajouter « Du contenu est partagé à partir de M365 » et choisir dans la liste « Avec des personnes externes à mon organisation ».

Dans Actions, ajouter une action « Restreindre l'accès ou chiffrer le contenu dans des emplacements M365 », puis cocher la case « Restreindre l'accès … » et choisir « Ne bloquez que les personnes extérieures à votre organisation ».

Dans notification aux utilisateurs, activer les notifications pour envoyer les conseils de stratégie. Vous pouvez complètement personnaliser ces messages.

Cliquer sur enregistrer pour enregistrer la règle.

Ensuite, vous pouvez choisir de « Commencer par tester » la stratégie, l'appliquer directement ou la laisser désactivée. Il est fortement recommandé de commencer par tester !

Il faut savoir que ces règles DLP peuvent mettre quelques heures voire quelques jours à s'appliquer. Donc ne travaillez pas dans l'urgence sur ces stratégies.

En appliquant une stratégie sur Teams, les utilisateurs seront limités dans les discussions et dans les canaux.

Modifier le dictionnaire par défaut

La valeur des règles DLP est fortement dépendante de la qualité du dictionnaire utilisé. Le dictionnaire de base de Microsoft contient surtout des informations liées à la protection des données personnelles comme le numéro de sécurité sociale, les numéros de carte bancaire, les numéros de sécurité sociales … Il convient d'enrichir ce dictionnaire avec des données propres à votre entreprise.

Cet enrichissement se fait toujours dans la console conformité et dans le menu « Classification des données » :

https://compliance.microsoft.com/dataclassification?viewid=overview

Vous pouvez enrichir le dictionnaire soit en créant des types d'infos confidentielles ou en créant des classifieurs.

Pour les type d'infos confidentielles, vous pouvez ajouter des informations sensibles via :

- Une expression régulière,
- Une liste de mots clés
- Un dictionnaire de mots clés
- L'utilisation de fonctions fournies par Microsoft (func_fr_passport la fonction de vérification si l'entrée correspond à un numéro de passeport français).

Pour les classifieurs, vous pouvez définir un type de documents sensibles en téléchargeant des modèles (anonymisés de préférence) et Microsoft va analyser les documents pour créer un classifieur qui permettra de détecter les documents approchant.

Surveiller la conformité DLP des données hors M365

Le menu Connecteurs de données dans la console de conformité permet de définir des connecteurs vers des applications externes ou des réseaux sociaux et de les inclure dans votre gestion de conformité DLP.

Règles DLP avancées – CASB

Il est possible de créer des stratégies très avancées pour interdire certaines actions ou limiter les fuites de données. Ces stratégies sont créées via l'accès conditionnel :

https://portal.azure.com/#view/Microsoft_AAD_IAM/ConditionalAccessBlade/~/Policies

Vous pouvez par exemple créer une nouvelle stratégie pour bloquer l'envoi de fichiers pour les externes ou invités sur tous les produits M365 ou Teams.

La sécurisation ultime

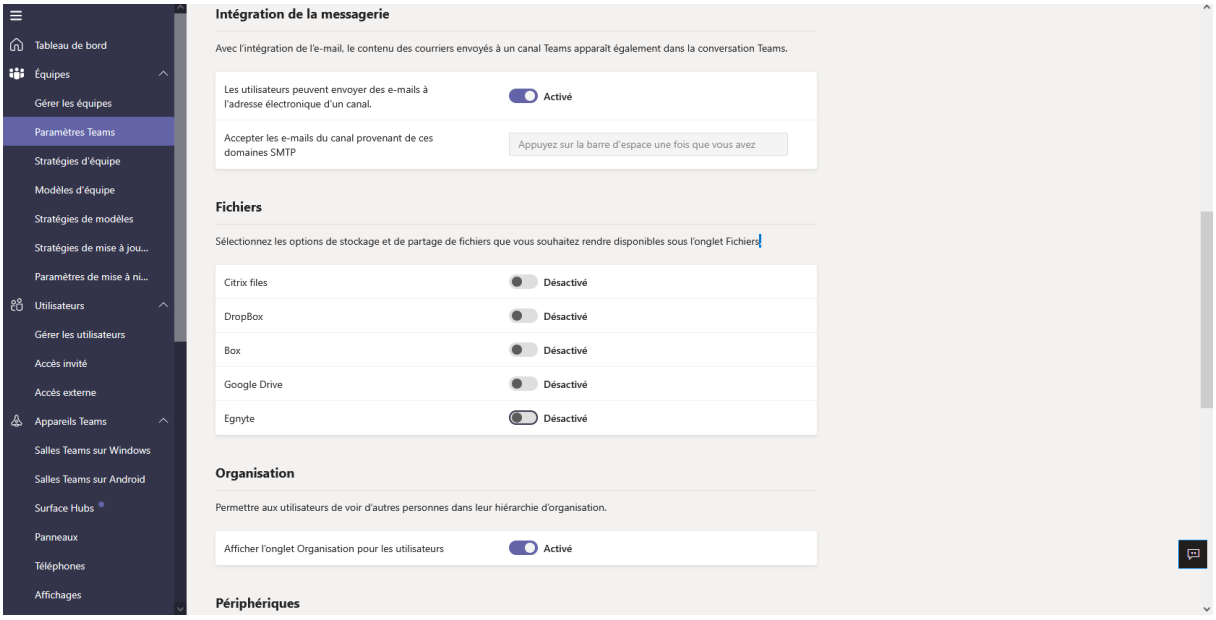
Si vous souhaitez aller plus loin dans la sécurisation et dans le bridage, vous pouvez supprimer les licences Sharepoint online et One drive pour chaque utilisateur et ils ne pourront plus stocker de documents dans Teams. Vous pouvez même supprimer toutes les fonctions collaboratives de Teams (équipes et canaux) et n'autoriser uniquement que les réunions.

Pour supprimer les licences Sharepoint online et Onedrive, allez dans la console Azure Active Directory et cliquer sur Users (Utilisateurs). Sélectionnez un ou plusieurs utilisateurs et cliquer sur licences dans le menu gauche. Cliquer sur le bundle (E1, E3, E5) et désactiver Sharepoint.

Il convient également de supprimer les solutions de stockage externe que l'on peut utiliser dans Teams dans les paramètres Teams :

https://admin.teams.microsoft.com/company-wide-settings/teams-settings

en désactivant Citrix files, dropbox, box, gooogle drive et Egnyte.



Vous pouvez restreindre également l'accès à la messagerie Exchange ou interdire les pièces jointes dans les messages à destination des destinataires externes. Attention de ne pas désactiver la licence Exchange car les utilisateurs n'auront plus le calendrier dans Teams !

La conclusion et les 10 commandements de la sécurisation de Teams

Pour conclure, Microsoft offre les outils pour sécuriser votre organisation M365 et plus particulièrement Teams. Dans une optique zéro-trust, soyez très restrictif et ouvrez en fonction des besoins.

Vous pouvez adapter vos besoins et aller relativement loin dans la sécurisation. Je vous conseille de faire constamment la balance entre la sécurité et les usages pour ne pas décevoir les utilisateurs par un bridage trop important.

Les 10 points qui me semblent importants sont :

1) Utiliser des comptes d'administration sans licence Teams
2) Définir l'organisation et la gouvernance des outils Azure et M365
3) MFA pour les administrateurs
4) Créer des stratégies Teams et les appliquer aux utilisateurs
5) Utiliser le tenant restriction v2 pour bloquer le mode anonyme et restreindre les tenants autorisés
6) Créer votre classification
7) Auto-classifier et positionner une étiquette par défaut restrictive
8) Contrôler et bloquer le partage de documents emails à l'extérieur de votre organisation
9) Enrichir les dictionnaires d'informations sensibles
10) Contrôler, auditer et alerter