Posture de l'appareil

Machine translated content

Disclaimer

Contents

Nouveautés

June 19, 2024

29 mai 2024

- **Disponibilité du service Device Posture en mode test - Technical Preview**

  Le service Device Posture est également disponible en mode test, permettant aux administrateurs de tester le service Device Posture avant de l'activer sur leur environnement de production. Les administrateurs peuvent ainsi analyser l'impact des analyses Device Posture sur les appareils des utilisateurs, puis planifier leur plan d'action en conséquence avant de l'activer en production. Pour plus de détails, consultez la section Service Device Posture en mode test - Technical Preview.

- **Analyse périodique des appareils - Technical Preview**

  Vous pouvez désormais activer l'analyse périodique des appareils Windows pour les contrôles configurés toutes les 30 minutes. Pour plus de détails, voir Analyse périodique des appareils - Technical Preview.

14 mai 2024

- **Ignorer les vérifications de posture des appareils**

  Les administrateurs peuvent autoriser les utilisateurs finaux à ignorer les contrôles Device Posture de leurs appareils. Pour plus de détails, voir Ignorer les contrôles Device Posture.

- **Tableau de bord du service Device Posture**

  Le portail du service Device Posture dispose désormais d'un tableau de bord affichant les journaux de surveillance et de dépannage. Les administrateurs peuvent désormais utiliser ce tableau de bord à des fins de surveillance et de dépannage. Pour plus de détails, consultez la section Journaux Device Posture.

- **Disponibilité générale des contrôles du navigateur et de l'antivirus**

  Les contrôles du navigateur et de l'antivirus sont désormais disponibles pour tous. Pour plus de détails, consultez la section Analyses prises en charge par le service Device Posture.

- **Disponibilité générale des messages personnalisés**

  L'option permettant d'ajouter des messages personnalisés lorsqu'un accès est refusé est désormais disponible pour tous. Pour plus de détails, consultez la section Messages personnalisés pour les scénarios d'accès refusé.

26 mars 2024

- **Prise en charge des URL d'espace de travail personnalisées**

  Les URL d'espace de travail personnalisées sont désormais prises en charge par le service Device Posture. Vous pouvez utiliser une URL qui vous appartient en plus de votre URL cloud.com pour accéder à Workspace. Assurez-vous d'autoriser l'accès à citrix.com depuis votre réseau. Pour plus de détails sur les domaines personnalisés, voir Configurer un domaine personnalisé.

12 février 2024

- **Prise en charge des contrôles du navigateur et de l'antivirus - Technical Preview**

  Le service Device Posture prend désormais en charge les contrôles du navigateur et de l'antivirus. Pour plus de détails, consultez la section Analyses prises en charge par le service Device Posture.

23 janvier 2024

- **Disponibilité générale de la vérification du certificat de l'appareil par le service Device Posture**

  La vérification du certificat de l'appareil à l'aide du service Device Posture est désormais disponible pour tous. Pour plus de détails, consultez la section Vérification du certificat de l'appareil avec le service Posture de l'appareil.

- **Caractéristiques préliminaires du service Posture de l'appareil**

  Le service Posture de l'appareil prend désormais en charge les contrôles suivants :

  - Le service Posture de l'appareil est désormais pris en charge sur les plateformes IGEL.
  - Le service Posture de l'appareil prend désormais en charge les vérifications de géolocalisation et de localisation réseau.

  Pour plus de détails, consultez la section Posture de l'appareil.

11 septembre 2023

- **Disponibilité générale de l'intégration de Posture de l'appareil avec Microsoft Intune**

  L'intégration de la posture des appareils à Microsoft Intune est désormais disponible pour tous. Pour plus de détails, consultez la section Intégration de Microsoft Intune à Posture de l'appareil.

30 août 2023

- **Gérer le client Citrix Endpoint Analysis pour le service Posture de l'appareil**

  Le client EPA peut être utilisé conjointement avec NetScaler et Posture de l'appareil. Certaines modifications de configuration sont nécessaires pour gérer le client EPA lorsqu'il est utilisé avec NetScaler et Posture de l'appareil. Pour plus de détails, consultez la section Gérer le client Citrix Endpoint Analysis pour le service Posture de l'appareil.

28 août 2023

- **Prise en charge du service Device Posture sur les plateformes iOS - Technical Preview**

  Le service Device Posture est désormais pris en charge sur les plateformes iOS. Pour plus de détails, consultez la section Posture de l'appareil.

22 août 2023

- **Vérification du certificat de l'appareil avec le service Citrix Device Posture - Technical Preview**

  Le service Citrix Device Posture peut désormais activer l'accès contextuel (Smart Access) aux ressources Citrix DaaS et Secure Private Access en vérifiant le certificat du terminal par rapport à une autorité de certification d'entreprise afin de déterminer si le terminal est fiable. Pour plus de détails, consultez la section Vérification du certificat de l'appareil avec le service Posture de l'appareil.

17 août 2023

- **Événements relatifs à la posture des appareils sur Citrix DaaS Monitor**

  Les événements du service Posture de l'appareil et les journaux de surveillance sont désormais consultables sur DaaS Monitor. Pour plus de détails, consultez la section Événements relatifs à la posture des appareils sur Citrix DaaS Monitor.

23 janvier 2023

- **Service de posture de l'appareil**

  Le service Citrix Posture de l'appareil est une solution basée sur le cloud qui aide les administrateurs à appliquer certaines exigences auxquelles les appareils finaux doivent satisfaire pour

accéder aux Citrix DaaS (applications et bureaux virtuels) ou aux ressources Citrix Secure Private Access (SaaS, applications Web, applications TCP et UDP). Pour plus de détails, consultez la section Posture de l'appareil.

[AAUTH-90]

- **Intégration de Microsoft Endpoint Manager à Posture de l'appareil**

  Outre les scans natifs proposés par le service Posture de l'appareil, le service Posture de l'appareil peut également être intégré à d'autres solutions tierces. Posture de l'appareil est intégré à Microsoft Endpoint Manager (MEM) sous Windows et macOS. Pour plus de détails, consultez la section Intégration de Microsoft Endpoint Manager à Posture de l'appareil.

  [ACS-1399]

Service Device Posture en mode test - Technical Preview

June 19, 2024

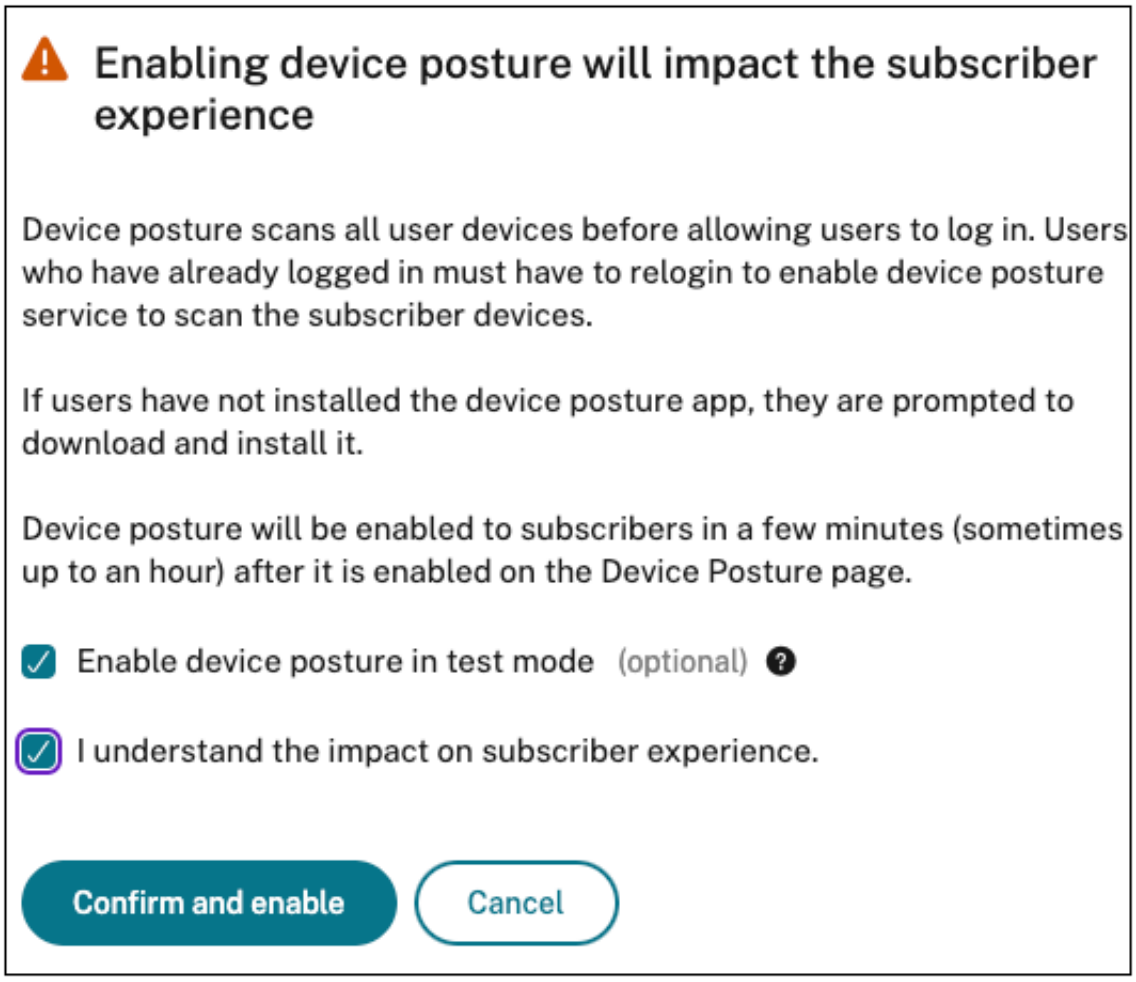
Le service Device Posture est également disponible en mode test, permettant aux administrateurs de tester le service Device Posture avant de l'activer sur leur environnement de production. Les administrateurs peuvent ainsi analyser l'impact des analyses Device Posture sur les appareils des utilisateurs, puis planifier leur plan d'action en conséquence avant de l'activer en production. Le service Device Posture en mode test collecte les données des appareils des utilisateurs finaux et classe les appareils dans les trois catégories suivantes : conformes, non conformes et refusés. Cependant, cette classification n'impose aucune action sur les appareils des utilisateurs finaux. Elle permet plutôt aux administrateurs d'évaluer leurs environnements et de renforcer la sécurité. Les administrateurs peuvent consulter ces données sur le tableau de bord Device Posture. Les administrateurs peuvent également désactiver le mode test, si nécessaire.

> **Remarque :**
>
> Le client EPA doit être installé sur les appareils. Si le client EPA n'est pas installé sur un terminal, le service Device Posture présente une page de téléchargement à l'utilisateur lui permettant de télécharger et d'installer le client, sans laquelle l'utilisateur ne peut pas se connecter.

Activer le mode test

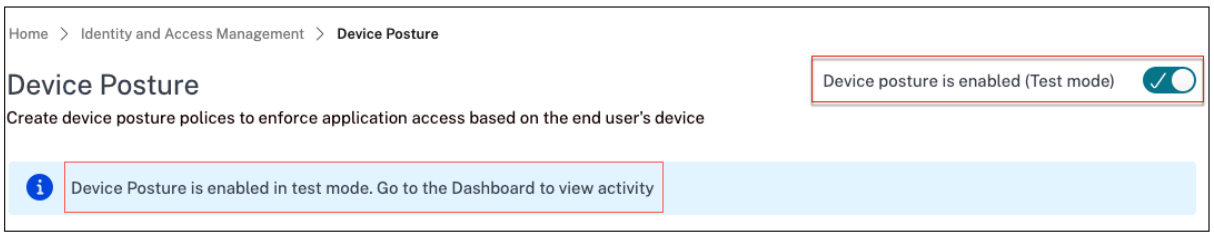
1. Connectez-vous à Citrix Cloud, puis sélectionnez **Gestion des identités et des accès** dans le menu hamburger.
2. Cliquez sur l'onglet **Device Posture**, puis sur **Gérer**.

3. Faites glisser le commutateur « **Device Posture désactivé** » sur ON.
4. Dans la fenêtre de confirmation, cochez les deux cases.



5. Cliquez sur **Confirmer et activer**.

Lorsque le service Device Posture est activé en mode test, la page d'accueil de Device Posture affiche une note le confirmant.



Les administrateurs peuvent configurer les stratégies et les règles relatives aux analyses de posture de l'appareil. Pour plus de détails, voir Configurer Device Posture. Sur la base des résultats de l'analyse, les appareils des utilisateurs finaux sont classés comme conformes, non conformes et refusés. Les administrateurs peuvent consulter ces données sur le tableau de bord.

Afficher les activités du mode test sur le tableau de bord

1. Cliquez sur l'onglet **Tableau de bord** sur la page Device Posture.

   Le graphique **des journaux de diagnostic** affiche le nombre d'appareils classés comme conformes, non conformes et dont la connexion a été refusée.

2. Pour afficher les détails, cliquez sur le lien **En savoir plus**.

Diagnostics en mode test

Les administrateurs peuvent télécharger les journaux de surveillance depuis l'interface utilisateur.

Activer le mode test en production

Si le service Device Posture est déjà activé en production, effectuez les étapes suivantes pour activer le mode test :

1. Sur la page d'accueil, faites glisser le commutateur « **Device Posture activé** » sur OFF.
2. Sélectionnez **Je comprends que tous les contrôles de posture de l'appareil seront désactivés**.
3. Cliquez sur **Confirmer et désactiver**.
4. Activez maintenant Device Posture en faisant glisser le commutateur **Device Posture désactivé** sur ON.
5. Dans la fenêtre de confirmation, sélectionnez les deux options suivantes.

   - **Activer Device Posture en mode test**
   - **Je comprends l'impact sur l'expérience des abonnés**

6. Cliquez sur **Confirmer et activer**.

Intégration de CrowdStrike à Device Posture

June 19, 2024

CrowdStrike Zero Trust Assessment (ZTA) fournit des évaluations de la posture de sécurité en calculant un score de sécurité ZTA compris entre 1 et 100 pour chaque appareil final. Un score ZTA plus élevé signifie que la posture de l'appareil final est meilleure.

Citrix Device Posture Service peut activer l'accès contextuel (Smart Access) aux ressources Citrix Desktop as a Service (DaaS) et Citrix Secure Private Access (SPA) en utilisant le score ZTA d'un appareil final.

Les administrateurs de Device Posture peuvent utiliser le score ZTA dans le cadre des stratégies et classer les terminaux comme conformes, non conformes (accès partiel) ou même refuser l'accès. Cette classification peut à son tour être utilisée par les organisations pour fournir un accès contextuel (Smart Access) aux applications et bureaux virtuels, ainsi qu'aux applications SaaS et Web. Les stratégies de score ZTA sont prises en charge pour les plates-formes Windows et macOS.

Configurer l'intégration CrowdStrike

La configuration de l'intégration de CrowdStrike est un processus en deux étapes.

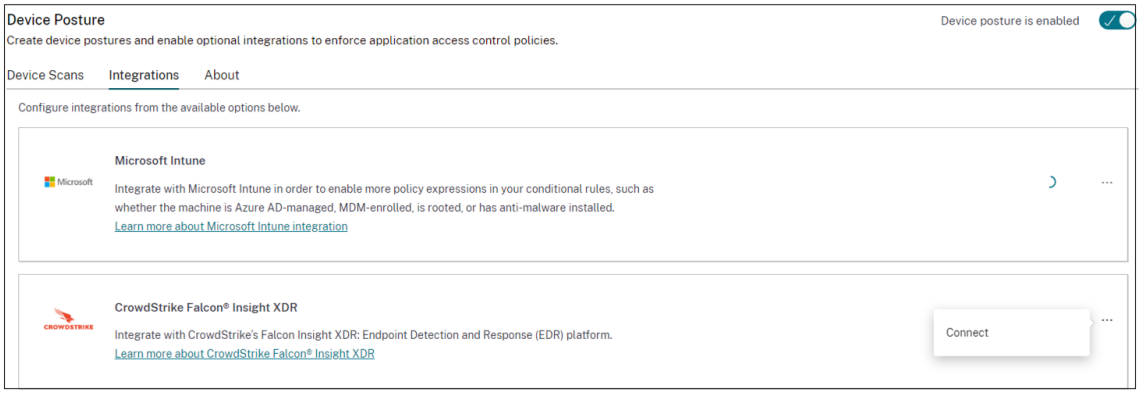
Étape 1 : établir un lien de confiance entre le service Citrix Device Posture et le service CrowdStrike ZTA. Il s'agit d'une activité ponctuelle.

Étape 2 : Configurez les stratégies pour utiliser le score ZTA de CrowdStrike comme règle afin de fournir un accès intelligent aux ressources Citrix DaaS et Citrix Secure Private Access.

Étape 1 : établir la confiance entre le service Citrix Device Posture et le service CrowdStrike ZTA

Effectuez les opérations suivantes pour établir la confiance entre le service Citrix Device Posture et le service CrowdStrike ZTA.

1. Connectez-vous à Citrix Cloud, puis sélectionnez **Identity and Access Management** dans le menu Hamburger.
2. Cliquez sur l'onglet **Device Posture** , puis sur **Gérer** .
3. Cliquez sur l'onglet **Intégrations** .



> **Remarque :**
>
> Les clients peuvent également accéder à l'option **Device Posture** dans le volet de navigation gauche de l'interface graphique du service Secure Private Access, puis cliquer sur l'onglet **Intégrations** .

4. **Cliquez sur le bouton représentant des points de suspension dans la zone CrowdStrike, puis sur Connect.** Le volet d'intégration de CrowdStrike Falco Insight XDR apparaît.
5. Entrez l'ID client et le secret client, puis cliquez sur **Enregistrer**.

> **Remarque :**
>
> - Vous pouvez obtenir l'ID client de l'API ZTA et le secret du client sur le portail CrowdStrike (**Support et ressources > Clients et clés d'API**).
> - Assurez-vous de sélectionner les étendues **Zero Trust Assessment** et **Host** avec des autorisations de lecture pour établir la confiance.

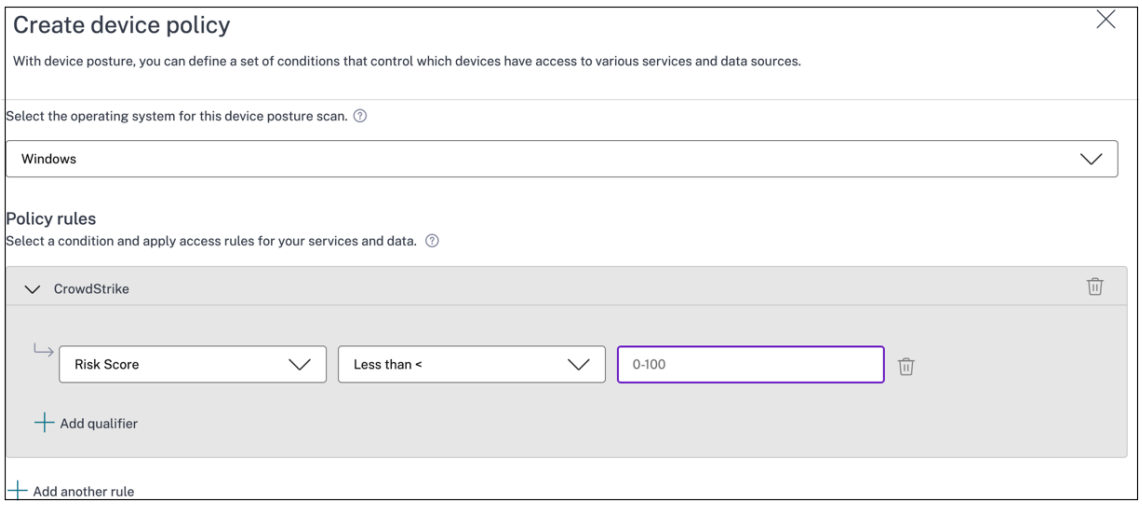
L'intégration est considérée comme réussie lorsque le statut passe de **Non configuré** à **Configuré** .

Si l'intégration échoue, le statut apparaît comme En **attente**. Vous devez cliquer sur le bouton en forme de point de suspension, puis sur **Reconnecter**.

Étape 2 : Configuration des stratégies d'état de sécurité de l'appareil

Procédez comme suit pour configurer les stratégies afin d'utiliser le score CrowdStrike ZTA comme règle afin de fournir un accès intelligent aux ressources Citrix DaaS et Citrix Secure Private Access.

1. Cliquez sur l'onglet **Analyses des appareils**, puis sur **Créer une stratégie relative aux appareils**.

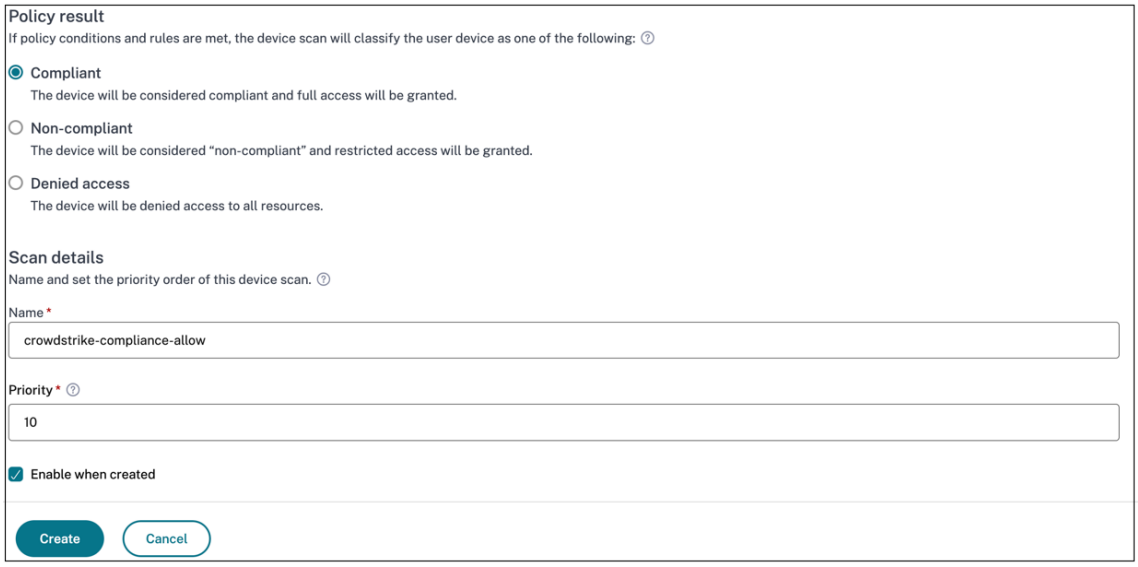


2. Sélectionnez la plateforme pour laquelle cette stratégie est créée.
3. Dans **Policy Rule**, sélectionnez **CrowdStrike**.
4. Pour le qualificatif du **score de risque** , sélectionnez la condition, puis saisissez le score de risque.
5. Cliquez sur **+** pour ajouter un qualificatif qui vérifie si le capteur CrowdStrike Falçon fonctionne.

> **Remarque :**
>
> Vous pouvez utiliser cette règle avec d'autres règles que vous configurez pour l'état de sécurité de l'appareil.

6. Dans **Résultat de la stratégie** basé sur les conditions que vous avez configurées, sélectionnez l'une des options suivantes.

   - **Conforme**
   - **Non conforme**
   - **Connexion refusée**



7. Entrez le nom de la stratégie et définissez la priorité.
8. Cliquez sur **Créer**.

Définitions

Les termes « conforme » et « non conforme » en référence au service Device Posture sont définis comme suit.

- Appareils conformes : appareil qui répond aux exigences des stratégies préconfigurées et qui est autorisé à se connecter au réseau de l'entreprise avec un accès complet ou illimité aux ressources Citrix Secure Private Access ou aux ressources Citrix DaaS.
- Appareils non conformes : appareil qui répond aux exigences des stratégies préconfigurées et qui est autorisé à se connecter au réseau de l'entreprise avec un accès partiel ou restreint aux ressources Citrix Secure Private Access ou aux ressources Citrix DaaS.

Références

Service Posture de l'appareil

Intégration de Microsoft Intune à Device Posture

June 19, 2024

Microsoft Intune classe l'appareil d'un utilisateur comme étant conforme ou enregistré en fonction de la configuration de sa stratégie. Lors de la connexion de l'utilisateur à Citrix Workspace, la position de l'appareil peut vérifier auprès de Microsoft Intune l'état de l'appareil de l'utilisateur et utiliser ces informations pour classer les appareils dans Citrix Cloud comme étant conformes, non conformes (accès partiel), ou même refuser l'accès à la page de connexion de l'utilisateur. Des services tels que Citrix DaaS et Citrix Secure Private Access utilisent à leur tour la classification des appareils selon la position des appareils pour fournir un accès contextuel (Smart Access) aux applications et bureaux virtuels, ainsi qu'aux applications SaaS et Web, respectivement.

Pour configurer l'intégration à Microsoft Intune

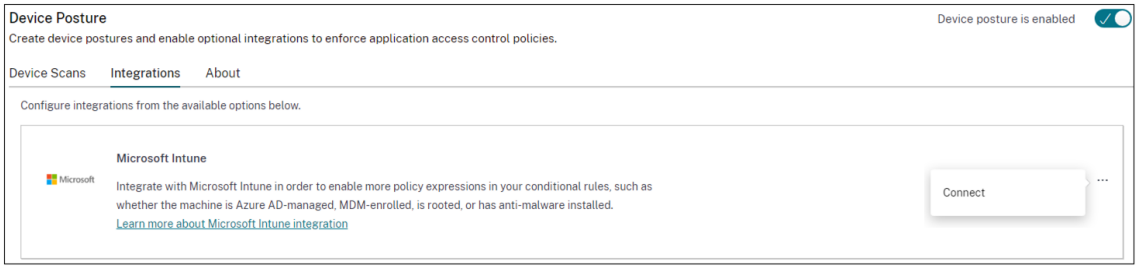
La configuration de l'intégration Intune est un processus en deux étapes.

Étape 1 : Intégrez la posture de l'appareil au service Microsoft Intune. Il s'agit d'une activité ponctuelle que vous effectuez pour établir un lien de confiance entre Device Posture et Microsoft Intune.

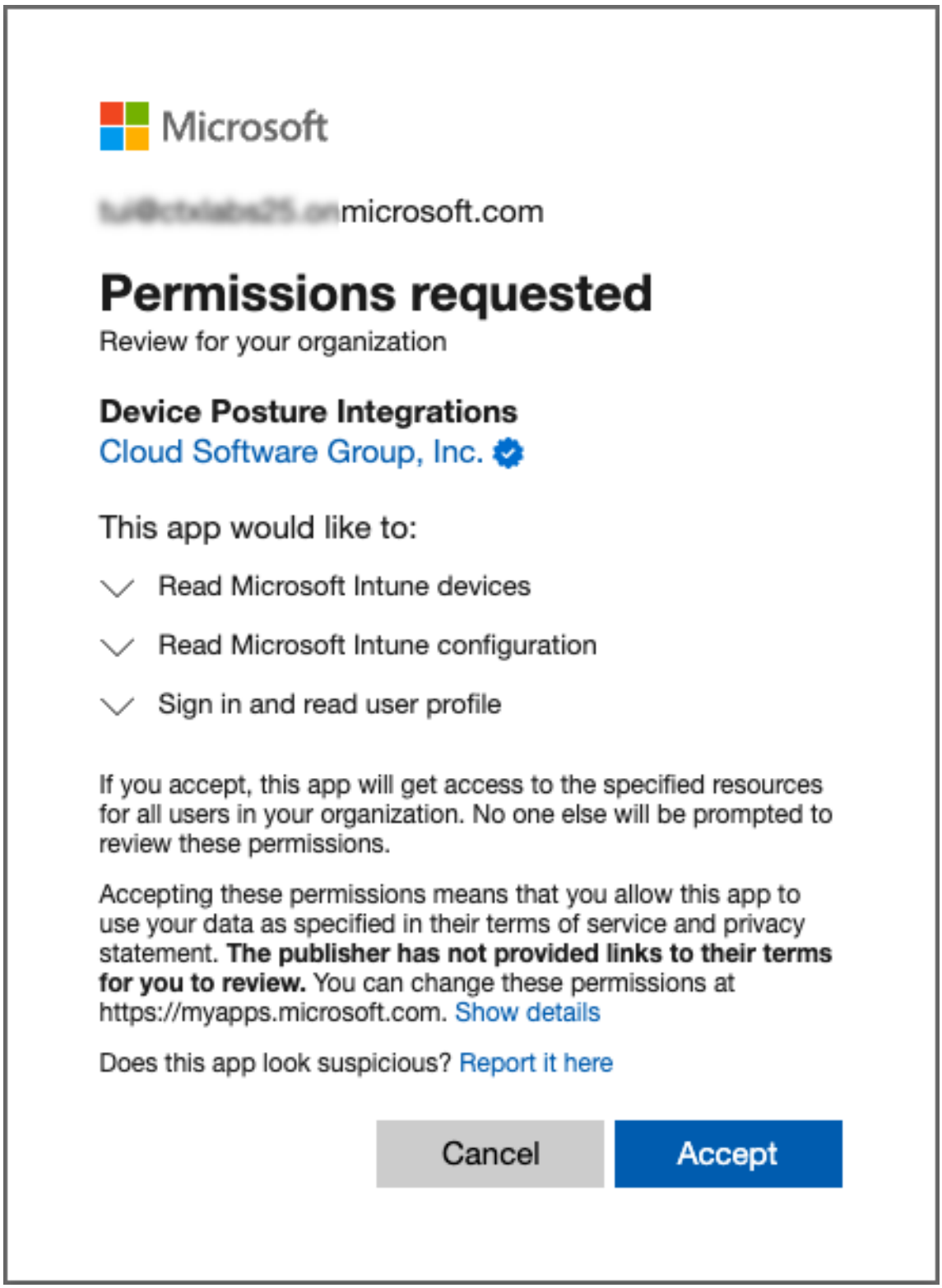
Étape 2 :configurez les stratégies pour utiliser les informations de Microsoft Intune.

Étape 1 : Intégrer la posture de l'appareil à Microsoft Intune

1. Pour accéder à l'onglet **Intégrations**, utilisez l'une des méthodes suivantes :
    - Accédez à l'URL https://device-posture-config.cloud.com dans votre navigateur, puis cliquez sur l'onglet **Intégrations** .
    - Clients de Secure Private Access : dans l'interface graphique de Secure Private Access, dans le volet de navigation de gauche, cliquez sur **Device Posture,** puis sur l'onglet **Intégrations** .



2. Cliquez sur le **bouton représentant trois points**, puis sur **Connecter**. L'administrateur est redirigé vers Azure AD pour s'authentifier.



Le tableau suivant répertorie les autorisations de l'API Microsoft Intune pour l'intégration au service Device Posture.

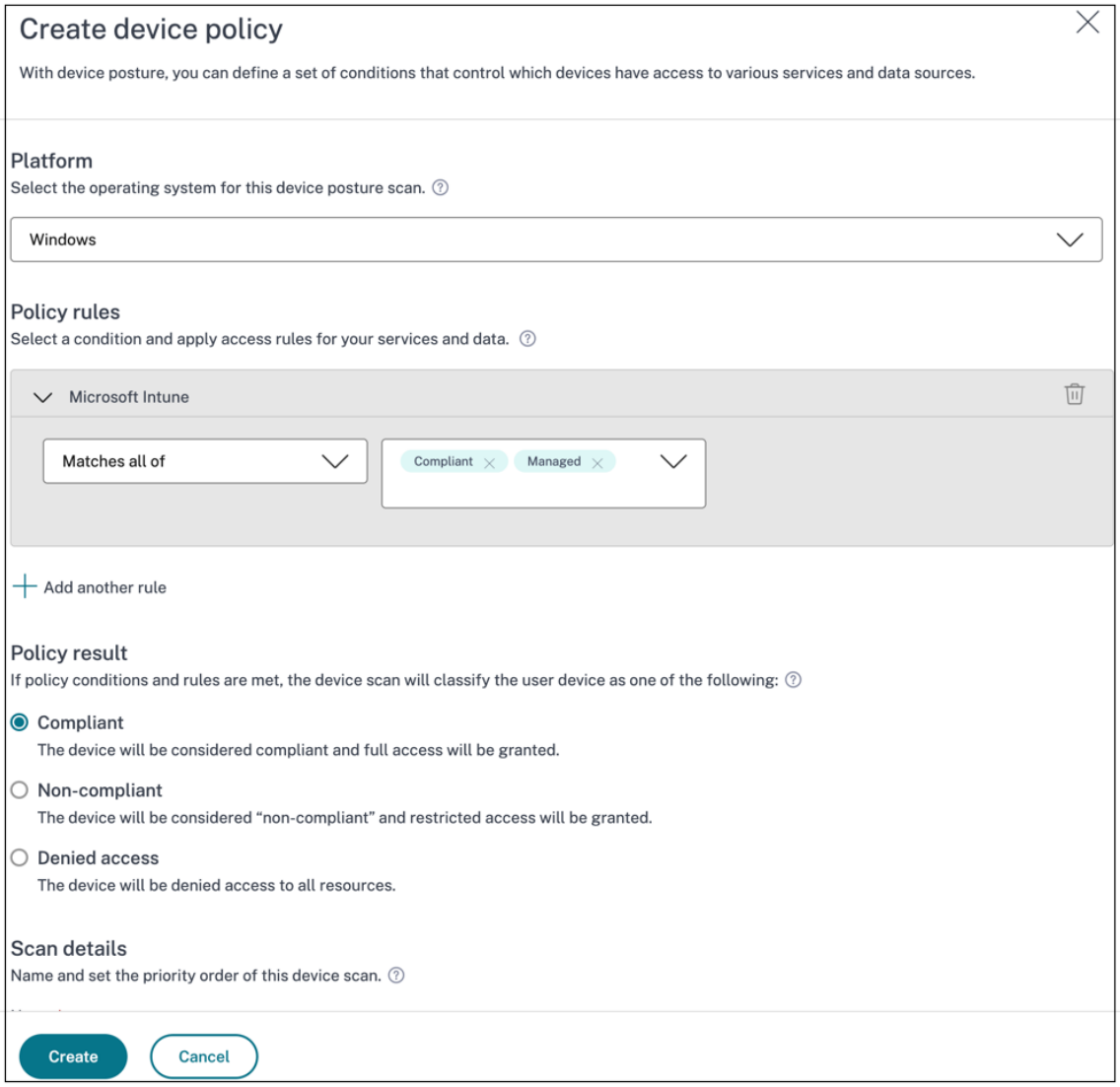
Nom de l'API	Valeur de la revendication	Nom de l'autorisation	Type
Microsoft Graph	DeviceManagementManagedDevices.Read.All	Lire les appareils Microsoft Intune	Application
Microsoft Graph	DeviceManagementServiceConfig.Read.All	Lire la configuration des appareils Microsoft Intune	Application

Lorsque le statut d'intégration passe de **Non**configuré à Configuré**, les administrateurs peuvent créer une stratégie d'état de sécurité de l'appareil.

Si l'intégration échoue, le statut apparaît comme En **attente**. Vous devez cliquer sur **les points, le bouton,** puis sur **Reconnecter**.

Étape 2 : Configuration des stratégies d'état de sécurité de l'appareil

1. Cliquez sur l'onglet **Analyses des appareils**, puis sur **Créer une stratégie relative aux appareils**.



2. Entrez le nom de la stratégie et définissez la priorité.
3. Sélectionnez la plateforme pour laquelle cette stratégie est créée.
4. Dans **Sélectionner une règle**, sélectionnez **Microsoft Endpoint Manager**.
5. Sélectionnez une condition, puis sélectionnez les balises MEM à associer.

    - **Pour chaque correspondance**, une condition OR est appliquée.
    - **Pour Correspond à tous**, une condition AND est appliquée.

    > **Remarque :**
    >
    > Vous pouvez utiliser cette règle avec d'autres règles que vous configurez pour l'état de sécurité de l'appareil.

6. Dans **Alors l'appareil est :** en fonction des conditions que vous avez configurées, sélectionnez l'une des options suivantes.

- **Conforme (un accès complet est accordé)**
- **Non conforme (accès restreint accordé)**
- **Connexion refusée**

Pour plus de détails sur la création d'une stratégie, voir Configurer la stratégie d'état de sécurité de l'appareil.

Vérification du certificat de l'appareil avec le service Device Posture

June 19, 2024

Pour configurer la vérification des certificats de l'appareil avec le service Posture de l'appareil, les administrateurs doivent importer un certificat émetteur depuis leur appareil. Une fois qu'un certificat émetteur valide est présent dans le service Posture de l'appareil, les administrateurs peuvent utiliser les vérifications des certificats des appareils dans le cadre des stratégies de posture des appareils.

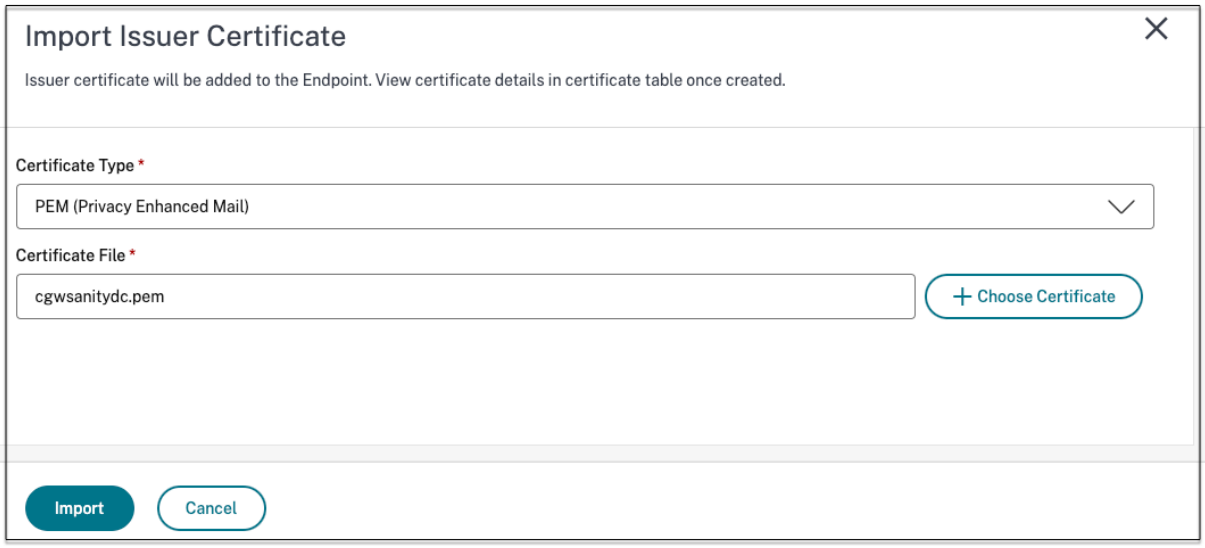
> **Points à noter :**
>
> - Le service Posture de l'appareil ne prend en charge que le type de certificat d'émetteur PEM.
> - Pour la vérification du certificat de l'appareil sous Windows, le client EPA du terminal doit être installé avec des droits d'administration. Pour les autres contrôles, vous n'avez pas besoin des droits administratifs locaux. Pour plus de détails sur les scans pris en charge, voir Scans pris en charge en fonction de la position de l'appareil.
> - Pour installer le client EPA avec des droits d'administration sous Windows, exécutez la commande suivante à l'emplacement où le plug-in client EPA est téléchargé.
>
>   ```
>   msiexec /i epasetup.msi
>   ```
>
> - La vérification du certificat de l'appareil avec le service Posture de l'appareil ne prend pas en charge la vérification de la révocation du certificat.
> - Si un certificat d'appareil est signé par un certificat intermédiaire, vous devez télécharger la chaîne complète contenant les certificats racine et intermédiaire dans un seul fichier PEM.
>
>   ```
>   Example: chain.pem
>
>   -----BEGIN CERTIFICATE-----
>   ******************************
>   -----END CERTIFICATE-----
>   -----BEGIN CERTIFICATE-----
>   ******************************
>   ```



```
-----END CERTIFICATE
```

Télécharger le certificat de l'appareil

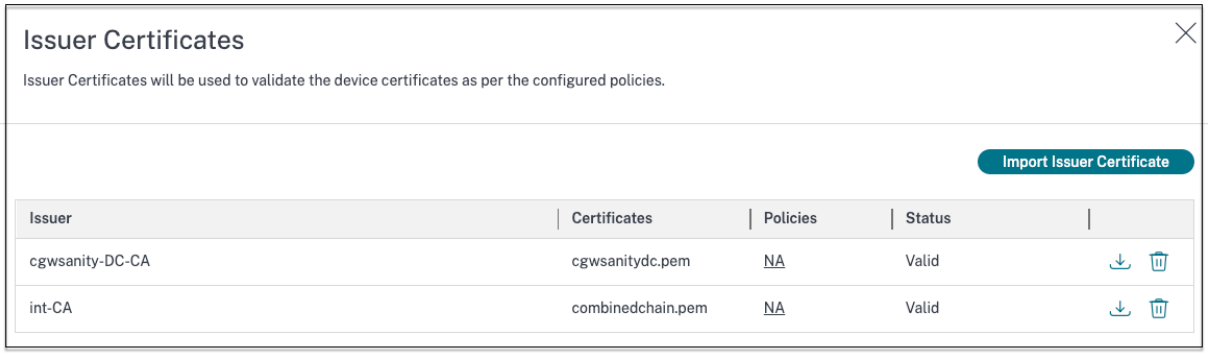
1. Cliquez sur **Paramètres** sur la page d'accueil de Posture de l'appareil.
2. Cliquez sur **Gérer**, puis sur **Importer un certificat de délivrance**.
3. Dans **Type de certificat**, sélectionnez le type de certificat. Seul le type PEM est pris en charge.
4. Dans **le fichier de certificat**, cliquez sur **Choisir un certificat** pour sélectionner le certificat de l'émetteur.
5. Cliquez sur **Ouvrir**, puis sur **Importer**.



Le certificat sélectionné est répertorié dans **Paramètres > Certificats d'émetteur.** Vous pouvez importer plusieurs certificats.

Afficher les certificats importés

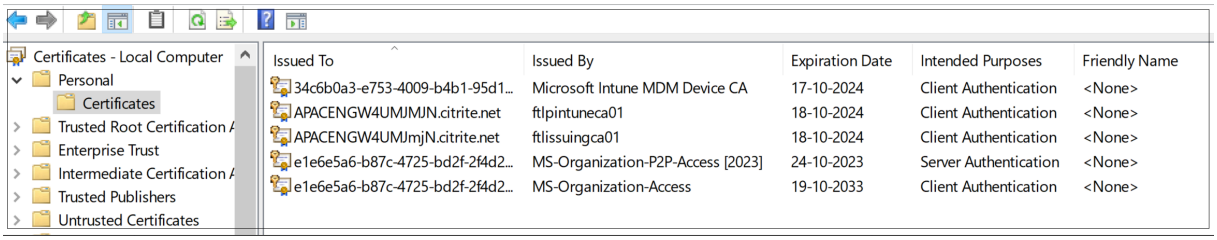
1. Cliquez sur **Paramètres** sur la page d'accueil de Posture de l'appareil.
2. Dans **Certificats d'émetteur**, cliquez sur **Gérer**.
3. La page Certificats d'émetteur répertorie les certificats d'émetteur importés.



Installer le certificat de l'appareil sur le terminal

Windows :

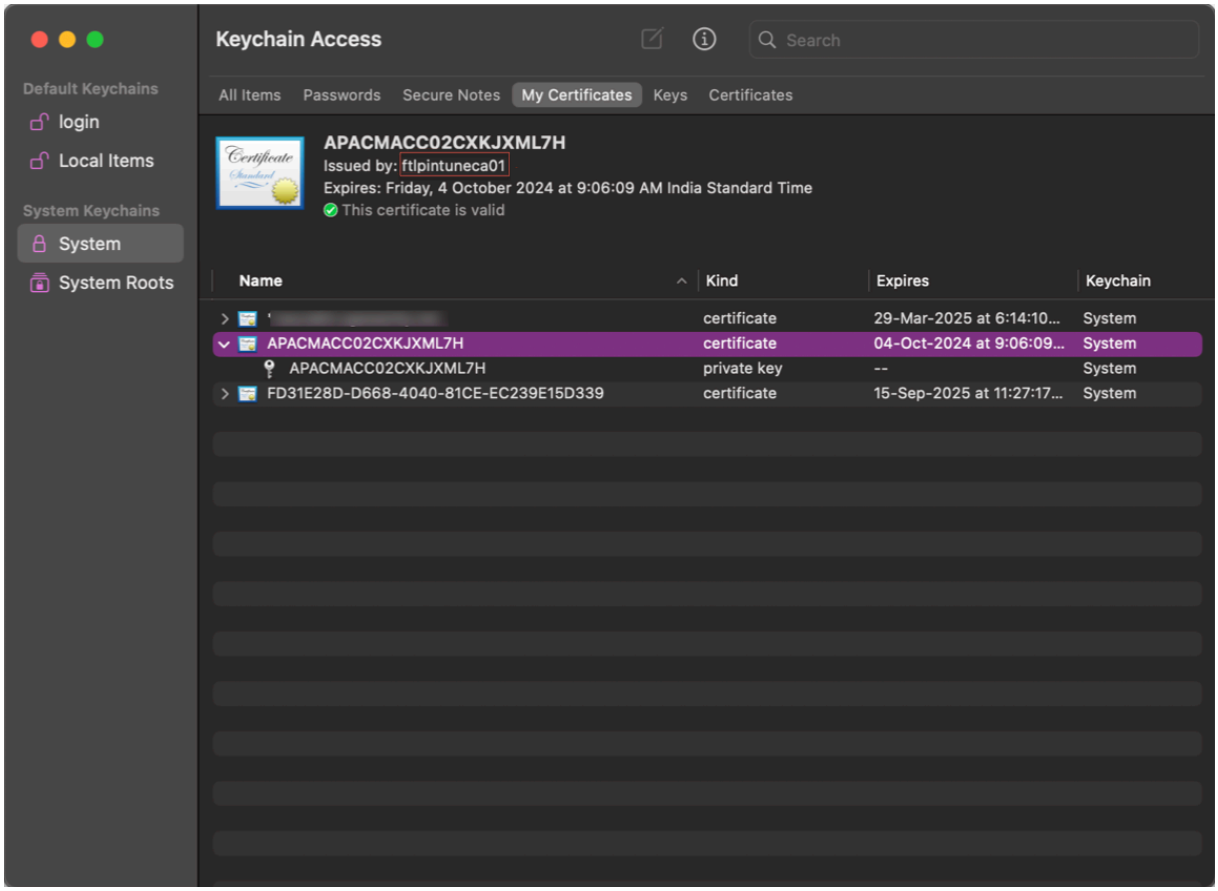
1. Dans le menu **Démarrer**, ouvrez **Computer Certificate Manager**.
2. Assurez-vous que le certificat est installé dans `Certificates - Local Computer\Personal\Certificates`.
   - Les **finalités prévues** doivent inclure l'**authentification du client**.
   - La colonne **Émis par** doit correspondre au nom de l'émetteur configuré sur l'interface graphique d'administration.



macOS :

1. Ouvrez **Keychain Access**, puis sélectionnez **Système.**
2. Cliquez sur **Fichier > Importer des éléments** pour importer le certificat.

   Le champ **Émis par** doit afficher le nom de l'émetteur du certificat.



Appliquez des contrôles intelligents sur les DaaS à l'aide de Posture de l'appareil

February 16, 2024

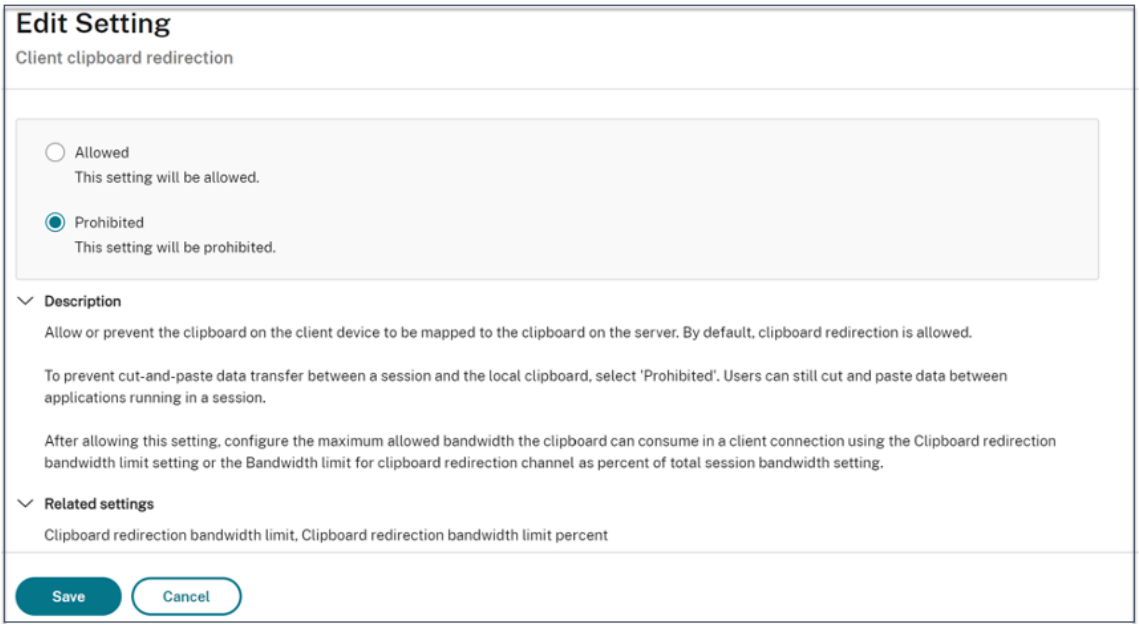
Vous pouvez appliquer des contrôles intelligents tout en accédant aux ressources Citrix Desktop as a Service (DaaS) via le service Citrix Posture de l'appareil.

> **Remarque :**
>
> il ne s'agit pas d'une configuration exhaustive, mais d'un exemple d'utilisation de Posture de l'appareil pour configurer les stratégies du Studio.

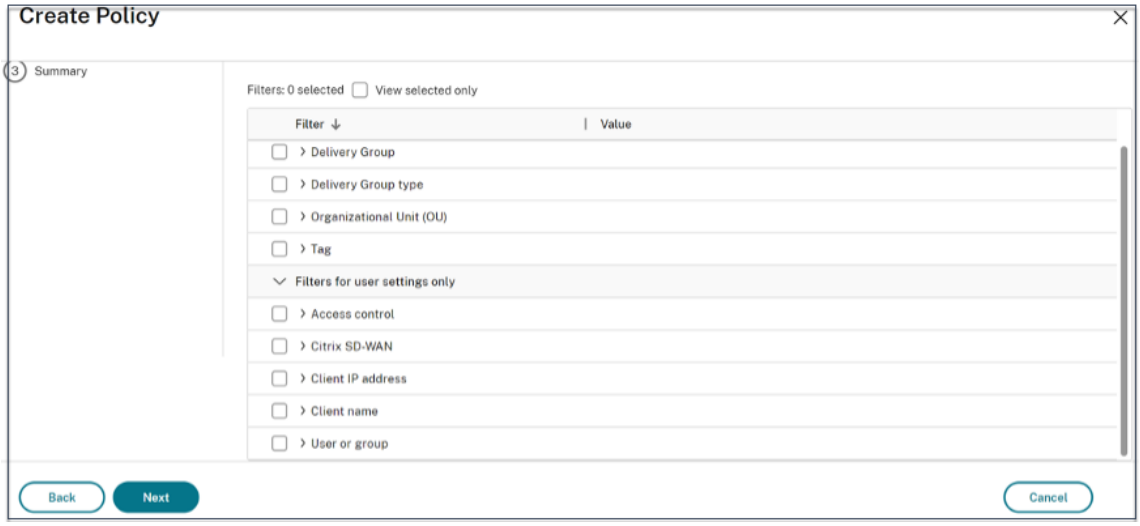
Dans cet exemple, une stratégie est créée pour désactiver la fonctionnalité copier-coller sur les ressources Citrix DaaS à l'aide des balises de service Posture de l'appareil (CONFORME et NON CONFORME).

Pour désactiver la fonctionnalité copier-coller pour les utilisateurs provenant d'un appareil NON CONFORME sur Citrix DaaS, effectuez les opérations suivantes :

1. Sur la page de configuration de Citrix DaaS, cliquez sur l'onglet **Gérer**.
2. Cliquez sur l'onglet **Stratégies**.
3. Sélectionnez **Créer une stratégie**.
4. Dans **Sélectionner les paramètres**, sélectionnez **Redirection du presse-papiers client**.
5. Dans **Modifier les paramètres**, sélectionnez **Interdit**, puis cliquez sur **Enregistrer**.

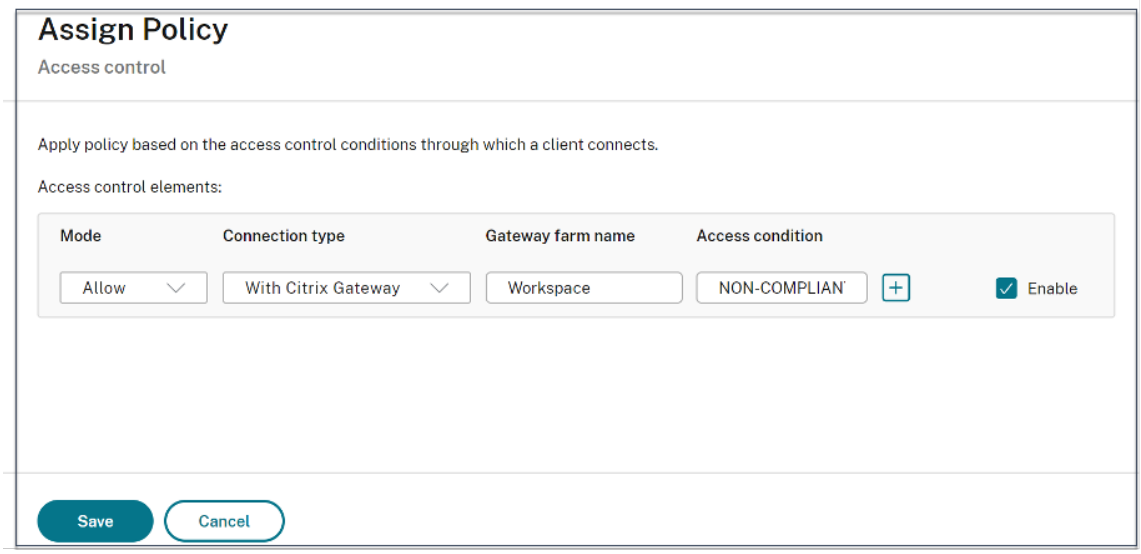


6. Sur la page **Utilisateurs et machines**, cliquez sur **Utilisateurs et ordinateurs filtrés**, puis attribuez cette stratégie au **contrôle d'accès**.
7. Accédez à **Filtrer pour les paramètres utilisateur uniquement** et sélectionnez **Contrôle d'accès**.



8. Sur la page **Attribuer une stratégie**, conservez les paramètres par défaut pour le **mode et letype de connexion**.

   Dans le **nom de la ferme Gateway**, saisissez **Workspace** et dans **Condition d'accès**, saisissez **NON CONFORME**.



9. Entrez un nom pour la stratégie. Envisagez de nommer la stratégie en fonction de la personne ou de l'objet concerné, par exemple, *accès restreint au Presse-papiers pour les appareils non conformes*. Facultativement, ajoutez une description.
10. Cliquez sur **Terminer.**

> **Remarque :**
>
> La stratégie est désactivée par défaut. L'activation de la stratégie permet de l'appliquer immédiatement aux utilisateurs qui se connectent. Si vous désactivez la stratégie, elle n'est pas appliquée. Si vous devez définir la priorité de la stratégie ou ajouter des paramètres ultérieurement, envisagez de désactiver cette stratégie jusqu'à ce que vous soyez prêt à l'appliquer.

Comment valider la configuration de votre stratégie

Validez vos stratégies pour vous assurer qu'elles fonctionnent comme prévu avant de les mettre en œuvre à grande échelle. Dans l'exemple de configuration :

- Pour les utilisateurs provenant d'un terminal CONFORME, les ressources Citrix DaaS doivent être énumérées sans les restrictions du copier-coller.
- Pour les utilisateurs provenant d'un terminal NON CONFORME, les ressources Citrix DaaS doivent être énumérées avec les restrictions de copier-coller.

Surveiller et résoudre les problèmes

June 19, 2024

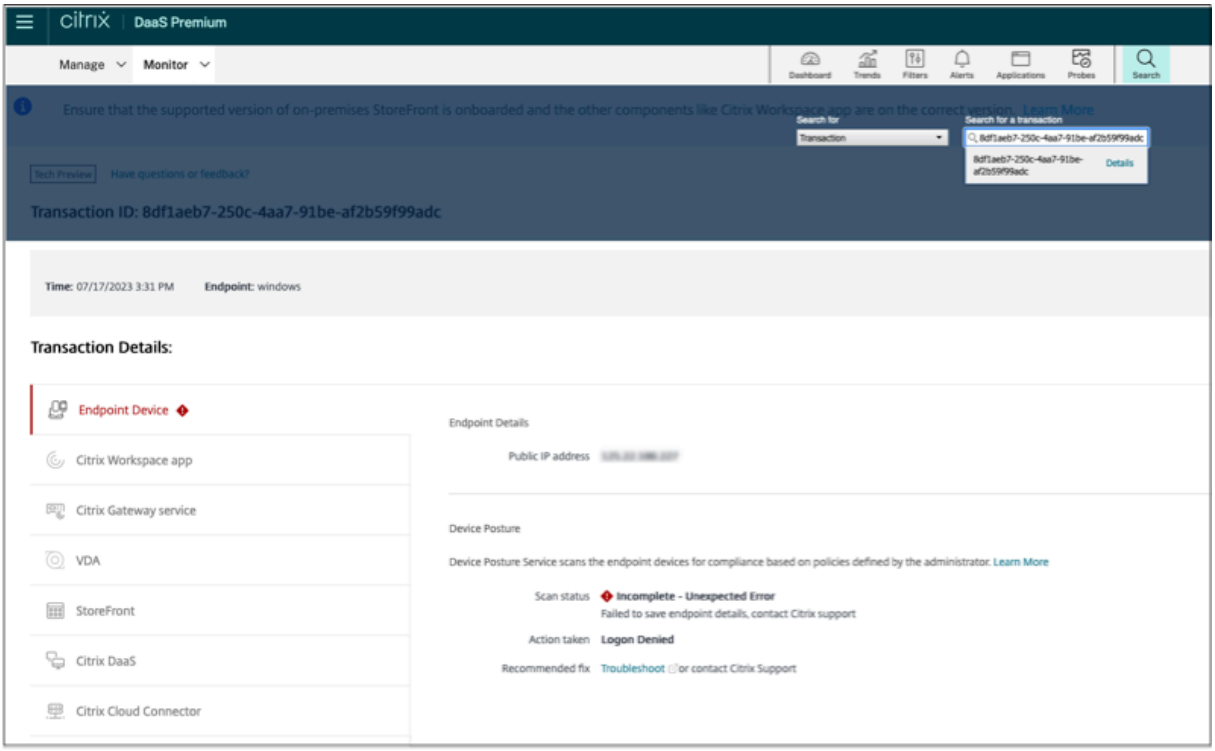
Les journaux des événements relatifs à la posture de l'appareil peuvent être consultés à deux endroits :

- Moniteur Citrix DaaS
- Tableau de bord Citrix Secure Private Access

Événements relatifs à la posture des appareils sur Citrix DaaS Monitor

Procédez comme suit pour consulter les journaux d'événements du service Posture de l'appareil.

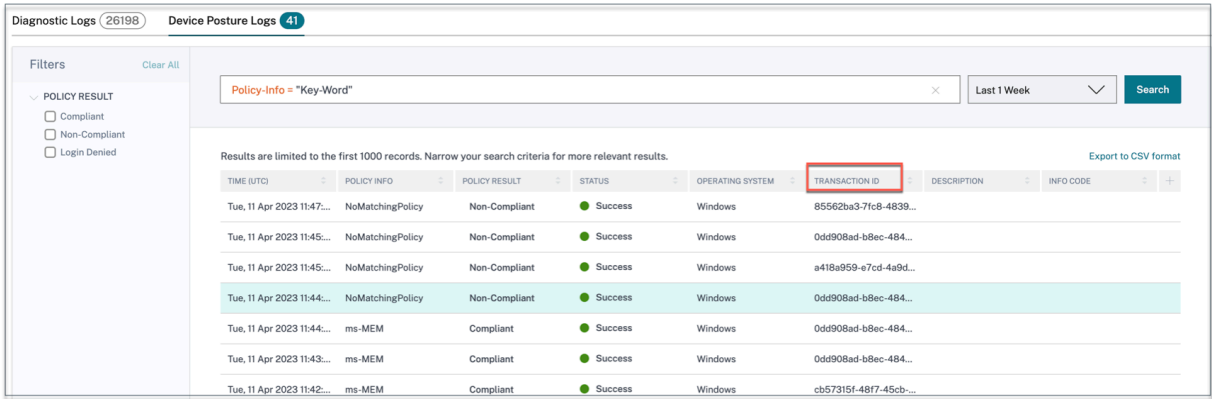
1. Copiez l'ID de transaction de la session ayant échoué ou dont l'accès a été refusé depuis la machine de l'utilisateur final.
2. Connectez-vous à Citrix Cloud.
3. Sur la vignette DaaS, cliquez sur **Gérer**, puis sur l'onglet **Surveiller** .
   Dans l'interface utilisateur de Monitor, recherchez l'ID de transaction à 32 chiffres et cliquez sur **Détails**.



Événements relatifs à la posture de l'appareil sur le tableau de bord Secure Private Access

Procédez comme suit pour consulter les journaux d'événements du service Posture de l'appareil.

1. Connectez-vous à Citrix Cloud.
2. Dans la vignette Secure Private Access, cliquez sur **Gérer**, puis sur **Tableau de bord**.
3. Cliquez sur le lien En **savoir plus** dans le graphique **des journaux de diagnostic** pour afficher les journaux des événements relatifs à la posture de l'appareil.



- Les administrateurs peuvent filtrer les journaux en fonction de l'ID de transaction figurant dans le graphique des journaux de diagnostic . L'ID de transaction est également affiché à l'utilisateur final chaque fois que l'accès est refusé.
- En cas d'erreur ou d'échec du scan, le service Posture de l'appareil affiche un identifiant de transaction. Cet ID de transaction est disponible dans le tableau de bord du service Secure Private Access. Si les journaux ne permettent pas de résoudre le problème, les utilisateurs finaux peuvent partager l'ID de transaction avec le support Citrix pour résoudre le problème.
- Les journaux du client Windows se trouvent à l'adresse suivante :
  - %localappdata%\Citrix\EPA\dpaCitrix.txt
  - %localappdata%\Citrix\EPA\epalib.txt
- Les journaux du client macOS peuvent être consultés à l'adresse suivante :
  - ~/Bibliothèque/Application Support/Citrix/EPAPlugin/EpaCloud.log
  - ~/Bibliothèque/Application Support/Citrix/EPAPlugin/epaplugin.log

Journaux d'erreurs de posture de l'appareil

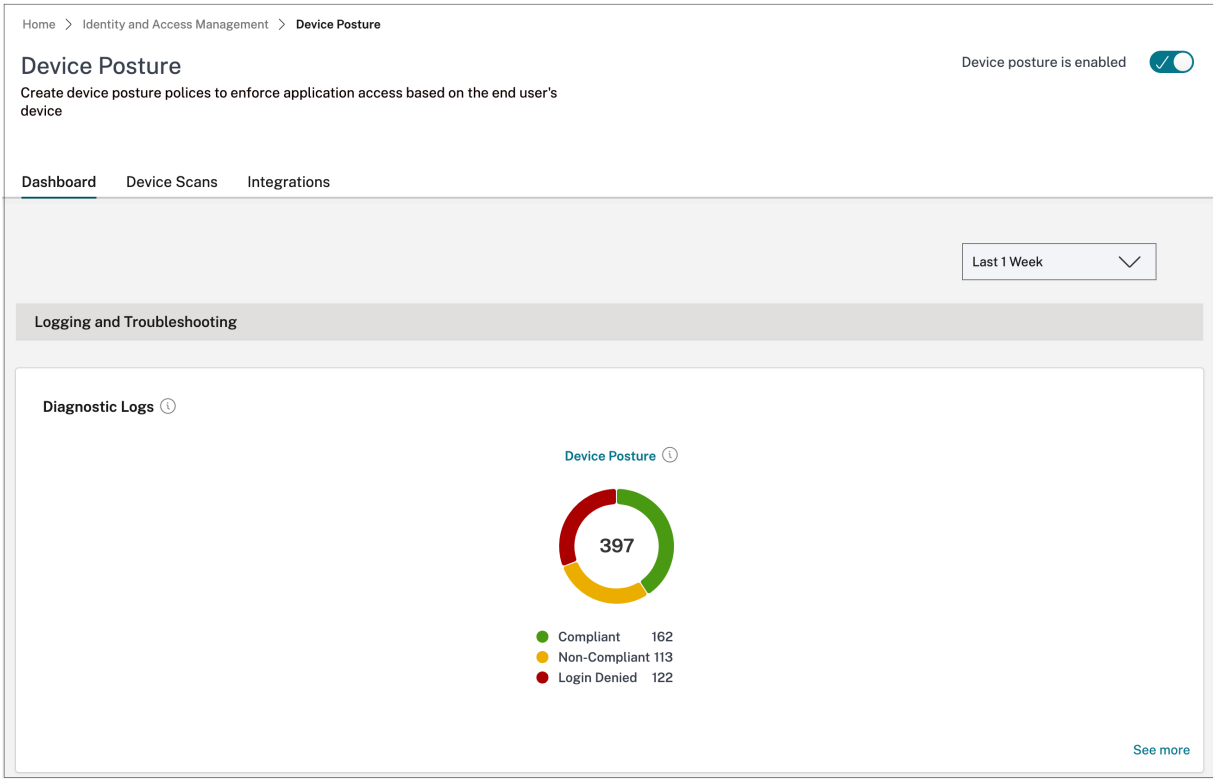
Les journaux suivants relatifs au service Posture de l'appareil peuvent être consultés sur le tableau de bord Citrix Monitor et Secure Private Access. Pour tous ces journaux, il est recommandé de contacter le support Citrix pour résoudre le problème.

- Impossible de lire les stratégies configurées
- Impossible d'évaluer les scans des terminaux
- Impossible de traiter les stratégies/expressions
- Impossible d'enregistrer les détails du terminal
- Impossible de traiter les résultats du scan à partir des terminaux

Journaux de posture de l'appareil

June 19, 2024

Vous pouvez utiliser le tableau de bord du portail de service Device Posture à des fins de surveillance et de dépannage. Pour afficher le tableau de bord du service Device Posture, cliquez sur l'onglet **Tableau de bord** sur la page d'accueil de Device Posture. La section **Journalisation et dépannage** affiche les journaux de diagnostic relatifs au service Device Posture. Vous pouvez cliquer sur le lien **Voir plus** pour afficher les détails des journaux. Vous pouvez affiner votre recherche en fonction des résultats de la stratégie (**conforme**, **non conforme**et **connexion refusée**).



> **Remarque :**
>
> Les journaux Device Posture sont également capturés dans le tableau de bord du service Secure

> Private Access. Pour afficher les journaux de posture de l'appareil, cliquez sur l'onglet **Journaux de posture de l'appareil** . Vous pouvez affiner votre recherche en fonction des résultats de la stratégie (**Conforme, Non conforme et connexion refusée**). Pour plus de détails, consultez la section Journaux de diagnostic.

Gérer le client Citrix Endpoint Analysis pour le service Device Posture

June 19, 2024

Le service Citrix Posture de l'appareil est une solution basée sur le cloud qui aide les administrateurs à appliquer certaines exigences auxquelles les appareils finaux doivent satisfaire pour accéder aux Citrix DaaS (applications et bureaux virtuels) ou aux ressources Citrix Secure Private Access (SaaS, applications Web, applications TCP et UDP).

Pour exécuter des analyses de position des appareils sur un appareil final, vous devez installer le client Citrix EndPoint Analysis (EPA), qui est une application légère, sur cet appareil. Le service Device Posture fonctionne toujours avec la dernière version du client EPA publiée par Citrix.

Installation du client EPA

Pendant l'exécution, le service Device Posture invite l'utilisateur final à télécharger et à installer le client EPA pendant l'exécution. Pour plus de détails, voir Flux d'utilisateurs finaux.
En général, un client EPA n'a pas besoin de droits d'administrateur local pour télécharger et installer sur un terminal. Toutefois, pour exécuter des scans de vérification des certificats d'appareils sur un appareil final, le client EPA doit être installé avec un accès administrateur. Pour plus de détails sur l'installation d'un client EPA avec accès administrateur, voir Installer un certificat de périphérique sur le terminal.

Mise à niveau du client EPA pour Windows

Lorsqu'une nouvelle version du client EPA est publiée, les clients EPA pour Windows sont mis à niveau par défaut après la première installation. La mise à niveau automatique garantit que les appareils des utilisateurs finaux fonctionnent toujours sur la dernière version du client EPA compatible avec le service Device Posture. Pour la mise à niveau automatique, le client EPA doit avoir été installé avec un accès administrateur.

> **Remarque :**
>
> la mise à niveau automatique est disponible en version Technical Preview. Inscrivez-vous à l'

> aperçu en utilisant https://podio.com/webforms/29214695/2384946.

Distribution du client de l'EPA

Les clients EPA peuvent être distribués à l'aide du service Global App Configuration (GACS) ou de l'EPA intégré au programme d'installation de l'application Citrix Workspace, ou à l'aide d'outils de déploiement de logiciels.

- **Programme d'installation du client EPA intégré à l'application Citrix Workspace :** Le programme d'installation du client EPA est intégré à l'application Citrix Workspace 2402 LTSR pour Windows. Cette intégration évite aux utilisateurs finaux d'installer le client EPA séparément après avoir installé l'application Citrix Workspace.

  Pour installer le client EPA dans le cadre de l'application Citrix Workspace, utilisez l'option de ligne de commande `InstallEPAClient`. Par exemple, `./CitrixworkspaceApp.exe InstallEPAClient`.

  > **Remarque :**
  >
  > - L'installation du client EPA dans le cadre de l'application Citrix Workspace est désactivée par défaut. Il doit être explicitement activé à l'aide de l'option de ligne de commande `InstallEPAClient`.
  > - Si un client EPA est déjà installé sur un terminal et que l'utilisateur final installe l'application Citrix Workspace, le client EPA existant est mis à niveau.
  > - Si un utilisateur final désinstalle l'application Citrix Workspace, le client EPA intégré est également supprimé de l'appareil, par défaut. Toutefois, si le client EPA n'a pas été installé dans le cadre de l'installation intégrée de l'application Citrix Workspace, le client EPA existant est conservé sur l'appareil.
  > - Le programme d'installation du client EPA intégré à l'application Citrix Workspace peut également être utilisé avec NetScaler. Pour plus de détails, voir Gérer le client EPA lorsqu'il est utilisé avec NetScaler et Device Posture.

- **Distribuez le client à l'aide de GACS** : GACS est une solution fournie par Citrix pour gérer la distribution des agents côté client (plug-ins). Le service de mise à jour automatique disponible dans le GACS garantit que les appareils finaux utilisent les dernières versions de l'EPA sans intervention de l'utilisateur final. Pour plus d'informations sur GACS, consultez Comment utiliser le service Global App Configuration.

> **Remarque :**
>
> - Le GACS est pris en charge sur les appareils Windows uniquement pour la distribution du client EPA.

> - Pour gérer un client EPA via GACS, installez l'application Citrix Workspace (CWA) sur les terminaux.
> - Si CWA est installé avec des privilèges d'administrateur sur un appareil d'utilisateur final, GACS installe le client EPA avec les mêmes privilèges d'administrateur.
> - Si CWA est installé avec des privilèges d'utilisateur sur un appareil d'utilisateur final, GACS installe le client EPA avec les mêmes privilèges d'utilisateur.

Distribuez le client à l'aide d'outils de déploiement de logiciels : le dernier client EPA peut être distribué par les administrateurs via des outils de déploiement de logiciels tels que Microsoft SCCM.

Gérez le client EPA lorsqu'il est utilisé avec NetScaler et Device Posture

Le client EPA peut être utilisé conjointement avec NetScaler et Device Posture dans les déploiements suivants :

- Authentification adaptative basée sur NetScaler avec EPA
- Passerelle sur site basée sur NetScaler avec EPA

Le service Device Posture transmet la dernière version du client EPA aux terminaux. Toutefois, sur NetScaler, les administrateurs peuvent configurer le contrôle de version suivant pour les scans EPA sur les serveurs virtuels de passerelle :

- **Toujours** : le client EPA sur l'appareil final et NetScaler doivent utiliser la même version.
- **Essentiel** : La version du client EPA sur le terminal doit se situer dans la plage configurée sur NetScaler.
- **Jamais** : l'appareil final peut avoir n'importe quelle version du client EPA.

Pour plus d'informations, consultez la section Comportements des plug-ins.

Considérations relatives à l'utilisation du client EPA avec NetScaler et Device Posture

Lorsqu'un client EPA est utilisé conjointement avec Device Posture Service et NetScaler, il peut arriver que l'appareil final exécute la dernière version du client EPA alors que NetScaler utilise une version différente du client EPA. Cela peut entraîner une incompatibilité entre la version du client EPA sur NetScaler et le périphérique final. Par conséquent, NetScaler peut inviter l'utilisateur final à installer la version du client EPA présente sur NetScaler. Pour éviter ce conflit, nous recommandons les modifications de configuration suivantes :

- Si vous avez configuré EPA avec l'authentification adaptative, l'authentification sur site ou le serveur virtuel de passerelle, il est recommandé de désactiver le contrôle de version du client EPA sur NetScaler. Ceci est fait pour s'assurer que le service GACS ou Device Posture ne transmet pas la dernière version du client EPA aux terminaux.

- Le contrôle de version de l'EPA peut être défini sur **Never** à l'aide de l'interface de ligne de commande ou de l'interface graphique. Ces modifications de configuration sont prises en charge sur NetScaler 13.x et versions ultérieures.
  - CLI : utilisez les commandes CLI pour l'authentification adaptative et le serveur virtuel d'authentification sur site.
  - Interface graphique : utilisez l'interface graphique du serveur virtuel de passerelle sur site. Pour plus de détails, consultez la section Contrôle de la mise à niveau des clients Citrix Secure Access.

Exemples de commandes CLI :

```
add rewrite action <rewrite_action_name> insert_http_header Plugin-
    Upgrade ""epa_win:Never;epa_mac:Always;epa_linux:Always;vpn_win:
    Never;vpn_mac:Always;vpn_linux:Always;""

add rewrite policy <rewrite_action_policy> "HTTP.REQ.URL.CONTAINS("
    pluginlist.xml")" <rewrite_action_name>

bind authentication vserver <Authentication_Vserver_Name> -policy <
    rewrite_action_policy> -priority 10 -type RESPONSE
<!--NeedCopy-->
```

Gouvernance des données

February 16, 2024

Cette rubrique fournit des informations concernant la collecte, le stockage et la conservation des journaux par le service Posture de l'appareil. Tous les termes en majuscules qui ne sont pas définis dans lessections Définitions ont la signification spécifiée dans leContrat de services de l'utilisateur final Citrix.

Résidence de données

Les données de contenu client de Citrix Posture de l'appareil se trouvent dans les services cloud AWS et Azure. Ils sont répliqués dans les régions suivantes à des fins de disponibilité et de redondance :

- AWS
  - États-Unis de l'Est
  - Inde occidentale
  - Europe (Francfort)

- Azure
  - États-Unis de l'Ouest
  - Europe de l'Ouest
  - Asie (Singapour)
  - Centre-sud des États-Unis

Vous trouverez ci-dessous les différentes destinations pour la configuration du service, les journaux d'exécution et les événements.

- Service Splunk pour la surveillance du système et les journaux de débogage, uniquement aux États-Unis.
- Citrix Analytics Service pour les diagnostics et les journaux d'accès utilisateur, consultez Citrix Analytics Service Data Governance pour plus d'informations.
- Service Citrix Cloud System Logs pour les journaux d'audit de l'administrateur. Pour plus de détails, consultez la section Gestion du contenu client et des journaux de Citrix Cloud Services et considérations géographiques.

Collecte des données

Le service Citrix Posture de l'appareil permet aux administrateurs clients de configurer le service via l'interface utilisateur Posture de l'appareil. Le contenu client suivant est collecté en fonction de la configuration de la stratégie de posture de l'appareil et de la plateforme :

- Version du système d'exploitation
- Version de l'application Citrix Workspace
- Adresses MAC
- Processus en cours
- Certificat de l'appareil
- Détails du registre
- Détails des mises à jour d'installation de Windows
- Détails de la dernière mise à jour Windows
- Système de fichiers : noms de fichiers, hachages de fichiers et heure de modification
- Nom de domaine

Pour les journaux d'exécution collectés par les composants de service, les informations clés sont les suivantes :

- Numéro du client/locataire
- ID de l'appareil (identifiant unique généré par Citrix)
- Sortie du scan de la posture de l'appareil
- Adresse IP publique du terminal

Transmission de données

Le service Citrix Posture de l'appareil envoie des journaux vers des destinations protégées par la sécurité de la couche transport.

Contrôle des données

Le service Citrix Posture de l'appareil ne propose actuellement aucune option permettant aux clients de désactiver l'envoi de journaux ou d'empêcher la réplication du contenu client à l'échelle mondiale.

Rétention des données

Selon la stratégie de rétention des données de Citrix Cloud, les données de configuration du client sont purgées du service 90 jours après l'expiration de l'abonnement.

Les destinations des journaux conservent leur stratégie de conservation des données spécifique au service.

- Pour plus de détails, consultez la section Gouvernance des données pour la stratégie de conservation des journaux Analytics.
- Les journaux Splunk sont archivés et finalement supprimés au bout de 90 jours.

Exportation de données

Il existe différentes options d'exportation de données pour différents types de journaux.

- Les journaux d'audit de l'administrateur sont accessibles depuis la console Citrix Cloud System Log.
- Les journaux de diagnostic du service Posture de l'appareil peuvent être exportés depuis le tableau de bord du service Citrix Analytics ou du service Secure Private Access sous forme de fichier CSV.

Définitions

- Le contenu client désigne toutes les données téléchargées sur un compte client à des fins de stockage ou les données dans un environnement client auquel Citrix a accès pour fournir des services.
- Un journal désigne un enregistrement des événements liés aux services, y compris des enregistrements qui mesurent les performances, la stabilité, l'utilisation, la sécurité et le support.

- Les services signifient que les services Citrix Cloud décrits précédemment aux fins de Citrix Analytics.