# Cylance Endpoint Security

## Guide de configuration

# Contents


## Configuration requise pour Cylance Endpoint Security..... 7
Configuration requise : console Cylance....7
Configuration requise : CylancePROTECT Desktop....7
Certificats racines requis pour l'agent CylancePROTECT Desktop pour Windows....12
Configuration requise : CylanceOPTICS....13
Configuration requise : application CylancePROTECT Mobile....17
Configuration requise : BlackBerry Connectivity Node....17
Configuration requise : connecteur CylanceGATEWAY....18
Configuration requise : agents CylanceGATEWAY....18
Configuration requise : CylanceAVERT....19
Configuration réseau requise pour Cylance Endpoint Security....19
Conditions requises pour le proxy Cylance Endpoint Security....25

## Connexion à la console de gestion.....27
Authentification personnalisée....27
Configurer l'authentification personnalisée....28
Descriptions de l'authentification personnalisée....28
Migration des IDP externes de l'authentification personnalisée vers un authentificateur....28
Authentification améliorée pour la connexion....29
Se connecter à la console de gestion Cylance Endpoint Security à l'aide de l'authentification améliorée....32
Générer une nouvelle URL de rappel SSO....33

## Configuration d'un nouveau locataire Cylance Endpoint Security.....34
Paramètres de configuration par défaut pour un nouveau locataire Cylance Endpoint Security....35
Exporter, importer ou réinitialiser la configuration d'un locataire Cylance Endpoint Security....39

## Installation de BlackBerry Connectivity Node.....41
Définir une variable d'environnement pour l'emplacement Java....41
Télécharger les fichiers d'installation et d'activation de BlackBerry Connectivity Node....42
Installer et configurer BlackBerry Connectivity Node....42
Copier les configurations de connexion au répertoire....44
Configurer des paramètres proxy pour une instance de BlackBerry Connectivity Node....44

## Association à votre annuaire d'entreprise..... 46
Configurer Cylance Endpoint Security pour la synchronisation avec EntraActive Directory....46
Mettre à jour les identifiants de connexion de Microsoft Entra ID Active Directory....47
Connexion à Microsoft Active Directory....48
Se connecter à un annuaire LDAP....49
Configurer l'intégration et la suppression....50
Configurer les plannings de synchronisation des annuaires....51
Synchroniser avec votre annuaire d'entreprise....52

**Configuration des administrateurs..... 53**
Ajouter un administrateur..... 53
Autorisations pour les rôles d'administrateur..... 54
Gestion des rôles..... 64
Ajouter un rôle..... 64
Configurer la limite d'expiration de session et d'expiration en cas d'inactivité..... 65

**Ajout d'utilisateurs et de terminaux..... 66**
Ajouter l'application CylancePROTECT Mobile et des utilisateurs CylanceGATEWAY..... 66
Ajout de groupes d'utilisateurs..... 67
Ajouter un groupe d'annuaires..... 68
Ajouter un groupe local..... 68
Ajouter un authentificateur..... 68
Considérations relatives à l'ajout d'authentificateurs SAML..... 80
Migrer des paramètres d'authentification personnalisés vers la liste des authentificateurs..... 81
Gérer les stratégies d'authentification pour votre locataire..... 83
Créer une stratégie d'authentification..... 84
Attribuer des stratégies à des administrateurs, des utilisateurs et des groupes..... 85
Classer les stratégies..... 86

**Inscription de CylancePROTECT Mobile et des utilisateurs CylanceGATEWAY..... 87**
Créer une stratégie d'inscription..... 87
Variables d'e-mail d'inscription prises en charge..... 88

**Configurer les zones pour gérer CylancePROTECT Desktop et CylanceOPTICS..... 90**
Ajouter et configurer une zone..... 90

**Configurer CylancePROTECT Desktop..... 93**
Test de votre déploiement CylancePROTECT Desktop..... 93
Créer une stratégie de test CylancePROTECT Desktop..... 94
Exclusions et quand les utiliser..... 96
Utiliser les stratégies de terminal pour gérer les terminaux CylancePROTECT Desktop..... 99
Créer et gérer une stratégie de terminal..... 100
Actions de fichier..... 101
Actions de mémoire..... 103
Paramètres de protection..... 113
Contrôle d'applications..... 120
Paramètres de l'agent..... 121
Contrôle de script..... 122
Contrôle du terminal..... 131
Installation de l'agent CylancePROTECT Desktop pour Windows..... 136
Installer l'agent Windows..... 136
Paramètres d'installation Windows..... 136
Installation de l'agent CylancePROTECT Desktop pour macOS..... 141

Installer l'agent CylancePROTECT Desktop sur macOS....141
Résolution des problèmes rencontrés lors de l'installation de macOS....145
Installation de l'agent CylancePROTECT Desktop pour Linux....147
Conditions préalables à l'installation sous Linux....148
Installer l'agent Linux automatiquement....150
Installer l'agent Linux manuellement....151
Mettre à niveau le pilote Linux....152
Commandes Linux de l'agent....155
Résolution des problèmes rencontrés lors de l'installation de l'agent Linux....156
Demander aux utilisateurs de fournir un mot de passe pour supprimer les agents CylancePROTECT Desktop et CylanceOPTICS....158

**Configurer CylancePROTECT Mobile....159**
Création d'une stratégie CylancePROTECT Mobile....159
Créer une stratégie d'évaluation des risques....162
Intégration d'Cylance Endpoint Security à Microsoft Intune pour répondre aux menaces mobiles....163
Connecter Cylance Endpoint Security à Intune....163
Utiliser les stratégies de protection des applications Intune avec CylancePROTECT Mobile....164

**Configurer CylanceOPTICS....165**
Installer l'agent CylanceOPTICSsur des terminaux....165
Configuration requise pour macOS 11.x et versions ultérieures....166
Commandes du système d'exploitation pour l'agent CylanceOPTICS....168
Activer et configurer CylanceOPTICS....171
Capteurs CylanceOPTICS....172
Capteurs CylanceOPTICS en option....173
Structures de données utilisées par CylanceOPTICS pour identifier les menaces....178

**Configurer CylanceGATEWAY....190**
Définition de votre réseau privé....191
Installation du connecteur CylanceGATEWAY....192
Spécifier votre réseau privé....210
Spécifier votre DNS privé....211
Spécifier vos suffixes DNS....212
Spécifiez les plages IP de l'agent privé CylanceGATEWAY....212
Apporter vos propres adresses IP (BYOIP)....213
Traduction d'adresses réseau avec CylanceGATEWAY....213
Définir des services réseau....213
Contrôle de l'accès réseau....214
Appliquer des règles ACL....215
Paramètres de l'ACL....216
Catégories de contenu de destination....219
Évaluer le niveau de risque d'une destination réseau....222
Configurer la liste de contrôle d'accès....222
Configurer la protection réseau....223
Seuil de risque de réputation de destination....224
Configurer les paramètres de protection réseau....225
Recherche de règles ACL et de services réseau....227
Utilisation de l'épinglage d'IP source....228
Configurer les options des services Gateway....228

Paramètres de stratégie de service Gateway..... 228
Configurer les options des services Gateway..... 235
Spécification de l'utilisation du tunnel CylanceGATEWAY par les terminaux activés avec une solution EMM..... 236
Connexion de Cylance Endpoint Security aux solutions MDM pour vérifier si les terminaux sont gérés..... 240
Conditions préalables : Vérifier que les terminaux sont gérés par MDM..... 241
Ajouter un connecteur BlackBerry UEM..... 243
Utiliser BlackBerry UEM pour installer l'application CylancePROTECT Mobile sur des terminaux..... 243
Connecter Cylance Endpoint Security à Intune..... 244
Installation de l‘agent CylanceGATEWAY..... 245
Effectuer une installation et une mise à niveau en mode silencieux de l‘agent CylanceGATEWAY..... 246

**Configurer CylanceAVERT..... 247**
Installation de l‘agent CylanceAVERT..... 247
Installer CylanceAVERT..... 248
Définir le contenu sensible à l‘aide des paramètres de protection des informations..... 248
Gérer la collecte de preuves..... 248
Ajouter des domaines autorisés et de confiance..... 249
Utiliser des modèles pour regrouper les types de données..... 250
Spécifier des types de données sensibles..... 251
Vérifier des domaines à l‘aide de certificats de confiance..... 252
Envoyer des notifications à des adresses e-mail spécifiées..... 253
Gérer des stratégies de protection des informations..... 253
Appliquer les bonnes pratiques de consolidation des règles..... 253
Créer un profil de protection des informations..... 254

**Gérer les mises à jour pour les agents CylancePROTECT Desktop et CylanceOPTICS..... 257**
Gérer les mises à jour pour les agents CylancePROTECT Desktop et CylanceOPTICS..... 258

**Connexion de Cylance Endpoint Security à des services externes..... 260**
Intégration de Cylance Endpoint Security avec Okta..... 260
Conditions préalables pour l‘ajout d‘un connecteur Okta..... 261
Ajouter et configurer un connecteur Okta..... 261
Intégration de Cylance Endpoint Security avec Mimecast..... 262
Conditions préalables pour l‘ajout d‘un connecteur Mimecast..... 262
Ajouter et configurer un connecteur Mimecast..... 264

**Annexe : bonnes pratiques pour le déploiement de CylancePROTECT Desktop sur des machines virtuelles Windows..... 265**
Configuration requise et considérations relatives à l'utilisation de CylancePROTECT Desktop sur des machines virtuelles..... 265
Déployer CylancePROTECT Desktop sur des machines virtuelles..... 267
Mettre à jour CylancePROTECT Desktop sur des terminaux clonés..... 268

**Informations juridiques..... 269**

# Configuration requise pour Cylance Endpoint Security

Pour commencer à configurer Cylance Endpoint Security, consultez cette section et vérifiez que l'environnement de votre organisation répond à la configuration requise pour les fonctionnalités et les composants de la solution.

## Configuration requise : console Cylance

| Élément | Configuration requise |
| --- | --- |
| Navigateurs pris en charge | Dernière version de :<br>• Google Chrome (recommandé)<br>• Microsoft Edge<br>• Mozilla Firefox<br>**Remarque :** Si vous utilisez Firefox pour accéder à la console de gestion, n'utilisez pas le mode de navigateur privé, n'activez pas Supprimer les cookies et les données du site lorsque Firefox est fermé et ne désactivez pas les employés du service. Toutes ces configurations peut entraîner un chargement de certains écrans de la console différent de celui attendu. |
| Langues prises en charge | Définissez votre navigateur sur l'une des langues prises en charge suivantes :<br>• Anglais<br>• Français<br>• Allemand<br>• Italien<br>• Japonais<br>• Coréen<br>• Portugais<br>• Espagnol |

## Configuration requise : CylancePROTECT Desktop

Pour plus d'informations sur les systèmes d'exploitation pris en charge par chacun des agents CylancePROTECT Desktop, reportez-vous à la Matrice de compatibilité Cylance Endpoint Security. Pour consulter les délais de prise en charge de tous les produits BlackBerry, consultez le Guide de référence du cycle de vie des logiciels BlackBerry Enterprise.

Les tableaux suivants répertorient les systèmes d'exploitation pris en charge qui présentent des exigences ou considérations supplémentaires. Notez que ces tableaux ne constituent pas une liste exhaustive des systèmes d'exploitation pris en charge. Si un système d'exploitation n'est pas répertorié dans les tableaux, cela signifie qu'il n'y a pas d'exigences ou de considérations supplémentaires.

**SE Windows**

| Système d'exploitation pris en charge | Configuration requise |
|---|---|
| Toutes les versions de système d'exploitation Windows prises en charge | • .NET Framework 4.6.2 ou version ultérieure<br>• TLS 1.2<br>• Pour connaître la configuration requise des machines virtuelles, les conseils de déploiement et les bonnes pratiques, reportez-vous à Annexe : bonnes pratiques pour le déploiement de CylancePROTECT Desktop sur des machines virtuelles Windows.<br>• CylancePROTECT Desktop ne prend pas en charge l'analyse des fichiers non hydratés depuis OneDrive Microsoft.<br>• Vérifiez que les dernières mises à jour de sécurité Windows ont été installées sur les terminaux avant d'installer ou de mettre à niveau l'agent CylancePROTECT Desktop. |
| Windows 11 (64 bits) | • Les systèmes de fichiers sensibles à la casse ne sont pas pris en charge.<br>• Les sessions multiples Windows 11 ne sont actuellement pas prises en charge. |
| Windows 10 (32 bits, 64 bits) | • Les systèmes de fichiers sensibles à la casse ne sont pas pris en charge.<br>• Les sessions multiples Windows 10 ne sont actuellement pas prises en charge.<br>• Windows 10 (v1809, mise à jour d'octobre 2018) : le filtre d'écriture unifié (UWF) n'est pas pris en charge. Désactivez UWF avant d'installer l'agent.<br>• Windows 10 (v1709, Fall Creators Update) : voir l'article KB 65647.<br>• Windows 10 Anniversary (v1607, Anniversary update) : il est recommandé de désactiver le sous-système Windows pour Linux. |
| Windows 7 (32 bits, 64 bits) | • Embedded Standard 7 et Embedded POSReady 7 sont pris en charge.<br>• Installez les certificats racine requis pour l'agent. |
| Windows Server 2022 (64 bits) | • Les éditions Standard, Data Center et Core sont prises en charge.<br>• Pour les éditions Data Center, l'agent ne prend pas en charge :<br>  • Rôle de serveur Hyper-V pour les machines virtuelles blindées<br>  • Prise en charge d'Hyper-V Host Guardian<br>  • Mise en réseau définie par logiciel<br>  • Storage Spaces Direct<br>• Storage Server 2022 n'est pas pris en charge. |

| Système d'exploitation pris en charge | Configuration requise |
| --- | --- |
| Windows Server 2019 (64 bits) | • Les éditions Standard, Data Center et Core sont prises en charge.<br>• Pour les éditions Data Center, l'agent ne prend pas en charge :<br>  • Rôle de serveur Hyper-V pour les machines virtuelles blindées<br>  • Prise en charge d'Hyper-V Host Guardian<br>  • Mise en réseau définie par logiciel<br>  • Storage Spaces Direct<br>• Storage Server 2019 n'est pas pris en charge. |
| Windows Server 2016 (64 bits) | • Les éditions Standard, Data Center, Essentials et Server Core sont prises en charge.<br>• Nano Server et Storage Server ne sont pas pris en charge. |
| Windows Server 2012 et 2012 R2 (64 bits) | • Les éditions Standard, Data Center, Essentials, Server Core, Embedded et Foundation sont prises en charge.<br>• Minimal Server Interface et Storage Server ne sont pas pris en charge. |

**macOS**

| Système d'exploitation pris en charge | Configuration requise |
| --- | --- |
| Toutes les versions macOS prises en charge | • TLS 1.2<br>• Vérifiez que les certificats racine suivants sont installés. Si ce n'est pas le cas, l'agent peut ne pas démarrer ou le terminal peut ne pas être en mesure de communiquer avec la console de gestion. Pour plus d'informations, consultez l'article KB 66608.<br>  • Autorité de certification publique principale de classe 3 VeriSign - G5<br>  • Thawte Primary Root CA<br>  • DigiCert Global Root<br>• Pour connaître la configuration requise des machines virtuelles, les conseils de déploiement et les bonnes pratiques, reportez-vous à Annexe : bonnes pratiques pour le déploiement de CylancePROTECT Desktop sur des machines virtuelles Windows.<br>• Les formats de volume sensibles à la casse ne sont pas pris en charge. |

| Système d'exploitation pris en charge | Configuration requise |
| --- | --- |
| macOS Sonoma (14) | • Reportez-vous à l'article KB 66578.<br>• Activez l'accès complet au disque. Si l'accès complet au disque n'est pas activé, CylancePROTECT Desktop ne peut pas traiter les fichiers sécurisés par la protection des données utilisateur. Pour plus d'informations, reportez-vous à l'article KB 66427.<br>• Reportez-vous à la section Résolution des problèmes rencontrés lors de l'installation de macOS.<br>• Les violations de protection de la mémoire suivantes sont prises en charge : Allocation à distance de la mémoire, Mappage à distance de la mémoire, Écriture à distance dans la mémoire, Annulation du mappage à distance de la mémoire. Les autres violations de la protection de la mémoire ne sont pas prises en charge pour Sonoma. |
| macOS Monterey (12) | • Reportez-vous à l'article KB 66578.<br>• Activez l'accès complet au disque. Si l'accès complet au disque n'est pas activé, CylancePROTECT Desktop ne peut pas traiter les fichiers sécurisés par la protection des données utilisateur. Pour plus d'informations, reportez-vous à KB66427.<br>• Reportez-vous à la section Résolution des problèmes rencontrés lors de l'installation de macOS.<br>• Les violations de protection de la mémoire suivantes sont prises en charge : Allocation à distance de la mémoire, Mappage à distance de la mémoire, Écriture à distance dans la mémoire, Annulation du mappage à distance de la mémoire. Les autres violations de la protection de la mémoire ne sont pas prises en charge pour Monterey. |
| macOS Big Sur (11) | • Reportez-vous à l'article KB 66578.<br>• Activez l'accès complet au disque. Si l'accès complet au disque n'est pas activé, CylancePROTECT Desktop ne peut pas traiter les fichiers sécurisés par la protection des données utilisateur. Pour plus d'informations, reportez-vous à l'article KB 66427.<br>• Reportez-vous à la section Résolution des problèmes rencontrés lors de l'installation de macOS.<br>• Les violations de protection de la mémoire suivantes sont prises en charge : Allocation à distance de la mémoire, Mappage à distance de la mémoire, Écriture à distance dans la mémoire, Annulation du mappage à distance de la mémoire. Les autres violations de la protection de la mémoire ne sont pas prises en charge pour Big Sur. |

**SE Linux**

| Système d'exploitation pris en charge | Configuration requise |
|---|---|
| Toutes les versions de système d'exploitation Linux prises en charge | • Une connexion Internet est requise. Si le terminal ne répond pas à cette exigence, envisagez la solution CylanceON-PREM plutôt.<br>• Consultez la feuille de calcul des noyaux Linux pris en charge.<br>• TLS 1.2<br>• Packages requis :<br>  • `bzip2(x86-64)`<br>  • `dbus-libs` (Pour RHEL/CentOS 7.x ou 8.x, la version 1.10.24 ou une version ultérieure est requise.)<br>  • `glibc`<br>  • `gtk3` (pour RHEL/CentOS)<br>  • `libgcc`<br>  • `openssl` (pour RHEL/CentOS 6.x)<br>  • `openssl-libs` (pour RHEL/CentOS 7.x)<br>  • `sqlite`<br>• Certificats racine :<br>  • Autorité de certification publique principale de classe 3 VeriSign - G5<br>  • Thawte Primary Root CA<br>  • DigiCert Global Root<br>• Versions GNOME prises en charge pour l'agent 2.1.1590 :<br>  • 3.28<br>  • 3.20<br>  • 3.14<br>  • 3.10<br>  • 3.8<br>• Les machines virtuelles sont prises en charge. |
| Ubuntu LTS 22.04 (64 bits)<br>Ubuntu LTS 20.04 (64 bits)<br>Ubuntu 20.04 (64 bits)<br>Ubuntu 18.04 (64 bits) | • Les noyaux Ubuntu Azure ne sont pas pris en charge.<br>• Utilisez le certificat d'autorité de certification de démarrage sécurisé CylancePROTECT Desktop pour prendre en charge le démarrage sécurisé UEFI. Pour en savoir plus, consultez l'article KB 73487. |
| Red Hat Enterprise Linux 9 (64 bits)<br>Red Hat Enterprise Linux/CentOS 8 (64 bits)<br>Red Hat Enterprise Linux/CentOS 7 (64 bits) | • Utilisez le certificat d'autorité de certification de démarrage sécurisé CylancePROTECT Desktop pour prendre en charge le démarrage sécurisé UEFI. Pour en savoir plus, consultez l'article KB 73487.<br>• FIPS est pris en charge. Pour obtenir des instructions sur l'activation du mode FIPS, reportez-vous à la documentation Red Hat de votre système d'exploitation. |

#### Utilisation de CylancePROTECT Desktop avec d'autres logiciels antivirus

Si un logiciel antivirus tiers est installé sur les terminaux dotés de CylancePROTECT Desktop, vous devrez peut-être effectuer des tâches de configuration supplémentaires pour vous assurer que ces produits n'interfèrent pas avec le fonctionnement de CylancePROTECT Desktop. Pour plus d'informations, consultez l'article KB 66448.

#### Spécifications matérielles

| Composant matériel | Configuration requise |
|---|---|
| Processeur (CPU) | Au moins deux cœurs de processeur qui :<br>• Prend en charge le jeu d'instructions SSE2<br>• Prend en charge le jeu d'instructions x86_64<br>• Prend en charge les processeurs d'Apple Silicon, dont M1, M2 et M3 ; nécessite Rosetta<br>• Ne prend pas en charge les instructions ARM définies pour Windows et Linux |
| Mémoire (RAM) | 2 Go |
| Espace disque (disque dur) | • 600 Mo<br>• L'utilisation de l'espace disque peut augmenter en fonction des fonctions activées (par exemple, définition du niveau de journalisation sur verbose) |

## Certificats racines requis pour l'agent CylancePROTECT Desktop pour Windows

Sur certaines versions de Windows, l'agent CylancePROTECT Desktop requiert les certificats racines suivants (voir Configuration requise : CylancePROTECT Desktop). Si des certificats racines sont manquants, l'agent risque de ne pas démarrer ou le terminal peut ne pas parvenir à communiquer avec la console de gestion. Pour plus d'informations sur les certificats racines manquants, consultez KB66608.

- Thawte Primary Root CA
- Thawte Timestamping CA
- Thawte Primary Root CA - G3
- Microsoft Root Certificate Authority 2010
- UTN-USERFirst-Object
- VeriSign Universal Root Certification Authority
- DigiCert High Assurance EV Root CA
- GlobalSign Root CA
- USERTrust RSA Certification Authority
- DigiCert Assured ID Root CA
- Autorité de certification publique principale de classe 3 VeriSign - G5
- DigiCert Global Root CA
- Starfield Class 2 Certification Authority

Pour plus d'informations, reportez-vous aux ressource suivantes :

- Thawte Root Certificates
- PKI Repository - Microsoft PKI Services
- DigiCert Roots and Intermediates
- DigiCert Trusted Root Authority Certificates

- GlobalSign Root Certificates
- Téléchargement et installation des certificats Sectigo Intermediate - RSA
- Obtain the VeriSign Class 3 Public Primary Certification Authority - G5 root certificate

# Configuration requise : CylanceOPTICS

**Agents**

| Agent | Configuration requise |
| --- | --- |
| Agent CylancePROTECT Desktop | • Vous devez installer l'agent CylancePROTECT Desktop sur un terminal avant d'installer l'agent CylanceOPTICS. L'agent CylanceOPTICS nécessite l'agent CylancePROTECT Desktop pour fonctionner.<br>• BlackBerry recommande d'installer la dernière version disponible de l'agent CylancePROTECT Desktop pour bénéficier des dernières fonctionnalités et des derniers correctifs.<br>• Pour l'agent CylanceOPTICS version 3.3, la version minimale requise de l'agent CylancePROTECT Desktop est 3.1.x. Si vous souhaitez utiliser les nouveaux capteurs Windows introduits dans CylanceOPTICS 3.3, la version minimale requise de l'agent CylancePROTECT Desktop pour Windows est 3.2.x.<br>• L'agent CylanceOPTICS versions 3.1 et 3.2 nécessite les versions minimales suivantes de l'agent CylancePROTECT Desktop :<br>  • Windows : 2.1.1578.x<br>  • macOS : 3.0.1000.x<br>  • Linux : 2.1.1590.x<br>• Consultez la matrice de compatibilité de CylancePROTECT Desktop et la configuration requise pour CylancePROTECT Desktop pour vérifier que vous installez un agent CylancePROTECT Desktop pris en charge et que vous répondez à toutes les autres exigences. |

| Agent | Configuration requise |
| --- | --- |
| Agent CylanceOPTICS | • BlackBerry recommande à d'installer la dernière version disponible de l'agent CylanceOPTICS sur chaque terminal.<br>• L'agent CylanceOPTICS 3.x ou une version ultérieure est nécessaire pour prendre en charge le stockage automatique des données collectées dans la base de données cloud CylanceOPTICS. Les versions antérieures de l'agent stockent les données CylanceOPTICS dans une base de données locale sur le terminal.<br>• Dans l'agent 3.x, les données collectées par les capteurs CylanceOPTICS sont mises en cache localement avant d'être envoyées à la base de données cloud CylanceOPTICS. Si le terminal est hors ligne, les données sont mises en cache jusqu'à ce que le terminal puisse se connecter à la base de données Cloud. Un maximum de 1 Go de données peut être stocké localement. Si plus de 1 Go de données sont stockées avant de pouvoir être téléchargées, les données de priorité la plus basse sont supprimées afin que les données de priorité supérieure puissent être mises en cache.<br>• Consultez les Notes de version Cylance Endpoint Security pour connaître les considérations relatives à la mise à niveau de l'agent CylanceOPTICS 2.x vers 3.x.<br>• Lorsque vous effectuez une mise à niveau de la version 2.x vers la version 3.x, le contenu complet de la base de données locale CylanceOPTICS est téléchargé par lots dans la base de données cloud.<br>• Une fois la mise à niveau vers la version 3.x effectuée, vous ne pouvez pas rétrograder l'agent vers la version 2.x. Si vous souhaitez installer la version 2.x, vous devez désinstaller la version 3.x, puis installer la version 2.x. |

#### Prise en charge du système d'exploitation et exigences supplémentaires

Pour plus d'informations sur les systèmes d'exploitation pris en charge par CylanceOPTICS, consultez la Matrice de compatibilité Cylance Endpoint Security. Pour connaitre les délais de prise en charge de tous les produits BlackBerry, consultez le Guide de référence du cycle de vie des logiciels BlackBerry Enterprise.

Le tableau suivant répertorie les systèmes d'exploitation pris en charge qui présentent des exigences ou considérations supplémentaires. Notez que ce tableau ne constitue pas une liste exhaustive des systèmes d'exploitation pris en charge. Si un système d'exploitation n'est pas répertorié dans le tableau, cela signifie qu'il n'y a pas d'exigences ou de considérations supplémentaires.

| OS | Configuration requise ou considérations |
| --- | --- |
| **Systèmes d'exploitation Windows** | |
| Windows 8.1<br>Windows 7 SP1 | Consultez cet article Microsoft pour connaître les dépendances supplémentaires pour la prise en charge de .NetCore. |
| **Systèmes d'exploitation macOS** | |

| OS | Configuration requise ou considérations |
|---|---|
| macOS Sonoma (14.x)<br>macOS Ventura (13.x)<br>macOS Monterey (12.x)<br>macOS Big Sur (11.x) | • Activez l'accès complet au disque. Pour plus d'informations, reportez-vous à l'article KB 66427.<br>• Reportez-vous à la section Configuration requise pour macOS 11.x et versions ultérieures. |
| macOS Catalina (10,15) | Activez l'accès complet au disque. Pour plus d'informations, reportez-vous à l'article KB 66427. |
| **Systèmes d'exploitation Linux** | |
| Tous les systèmes Linux pris en charge | • kernel-headers et kernel-devel sont requis, et la version doit correspondre au noyau en cours d'exécution. Au cours de l'installation, le gestionnaire de packages indique les versions requises. Pour les systèmes Ubuntu pris en charge et Debian, les entêtes Linux sont l'équivalent des entêtes kernel.<br>• L'une des suites de capteurs Linux suivantes est requise : eBPF, Netlink (avec prise en charge de la multidiffusion Netlink 3.16 ou version ultérieure, ou démon d'audit désinstallé) ou Auditdsp (avec les plug-ins auditd et auditdsp configurés pour s'activer au démarrage). EBPF est recommandé pour des performances optimales avec l'agent CylanceOPTICS. Si eBPF n'est pas disponible, l'agent tente d'utiliser Netlink pour obtenir le meilleur niveau de performances. Si Netlink n'est pas disponible, l'agent tente d'utiliser Auditdsp. Les suites de capteurs disponibles varient en fonction de la version de votre système d'exploitation. |
| RHEL/CentOS 8.x<br>RHEL/CentOS 7.x | • Pour RHEL/CentOS 8.x, ncurses-compat-libs est requis, sauf si les terminaux exécutent l'agent CylanceOPTICS version 3.2.1140-x ou versions ultérieures.<br>• Firewalld doit être activé et en cours d'exécution pour prendre en charge la fonction de verrouillage du terminal. Firewalld est disponible par défaut avec RHEL/CentOS. |
| Amazon Linux 2 | • ncurses-compat-libs est requis sauf si les terminaux exécutent l'agent CylanceOPTICS version 3.2.1140-15000 ou versions ultérieures.<br>• Firewalld doit être activé et en cours d'exécution pour prendre en charge la fonction de verrouillage du terminal. Firewalld doit être installé manuellement sur Amazon Linux 2. |
| Oracle Linux Server UEK 8 (64 bits)<br>Oracle Linux Server 8 (64 bits)<br>Oracle Linux Server 7 (64 bits)<br>Oracle Linux Server UEK 7 (64 bits) | • ncurses-compat-libs est requis sauf si les terminaux exécutent l'agent CylanceOPTICS version 3.2.1140-37000 ou versions ultérieures.<br>• Firewalld doit être activé et en cours d'exécution pour prendre en charge la fonction de verrouillage du terminal. Firewalld est disponible par défaut avec Oracle Linux. |

| OS | Configuration requise ou considérations |
|---|---|
| Ubuntu 22.04<br>Ubuntu 20.04<br>Ubuntu 18.04 | • Ubuntu 20.04 nécessite libtinfo5, sauf si les terminaux exécutent l'agent CylanceOPTICS version 3.2.1140-x ou versions ultérieures.<br>• Firewalld doit être activé et en cours d'exécution pour prendre en charge la fonction de verrouillage du terminal. Firewalld doit être installé manuellement pour Ubuntu. |
| SUSE Enterprise Linux 15 SP4<br>SUSE Enterprise Linux 15<br>SUSE Enterprise Linux 12 | • policycoreutils est nécessaire.<br>• Pour SUSE 15.x, kernel-default-devel doit correspondre au noyau. libncurses5 est également requis, sauf si les terminaux exécutent l'agent CylanceOPTICS version 3.2.1140-29000 ou versions ultérieures.<br>• Firewalld doit être activé et en cours d'exécution pour prendre en charge la fonction de verrouillage du terminal sur SUSE 15.x. Firewallld est disponible par défaut avec SUSE 15.x. La fonction de verrouillage de terminal n'est pas prise en charge pour SUSE 12. |
| Debian 11<br>Debian 10 | • Les terminaux Debian 10 nécessitent iptables 1.8.5 ou une version ultérieure pour prendre en charge la fonctionnalité de verrouillage du terminal.<br>• Firewalld doit être activé et en cours d'exécution pour prendre en charge la fonction de verrouillage du terminal. Firewalld doit être installé manuellement pour Debian. |

**Compatibilité avec d'autres solutions EDR**

L'agent CylanceOPTICS n'est pas compatible avec d'autres solutions EDR (Endpoint Detection and Response) installées sur le même terminal. Supprimez toutes les solutions EDR tierces d'un terminal avant d'installer et d'activer l'agent CylanceOPTICS.

**Matériel**

| Élément | Configuration requise |
|---|---|
| Processeur (CPU) | • En général, jusqu'à 1 % de CPU supplémentaire<br>• Pour les charges de travail intensives et soutenues, des pics de charge supplémentaires de 5 à 25 % peuvent être nécessaires, selon la charge de travail |
| Mémoire (RAM) | L'agent nécessite 0,2 à 1,0 Go de mémoire supplémentaire, selon la charge de travail. |
| Espace disque (disque dur) | Minimum 1 Go<br>• Pour l'agent 2.x CylanceOPTICS et les versions antérieures, 1 Go minimum sont requis pour la base de données locale.<br>• Pour CylanceOPTICS 3.0 et ultérieures, 1 Go minimum sont recommandés pour la mise en cache des données du capteur CylanceOPTICS avant que le terminal puisse télécharger les données dans la base de données cloud CylanceOPTICS lorsqu'il est en ligne. |

### Machines virtuelles

CylanceOPTICS est pris en charge pour les machines virtuelles. Pour connaître la configuration requise, les conseils de déploiement et les bonnes pratiques, reportez-vous à Annexe : bonnes pratiques pour le déploiement de CylancePROTECT Desktop sur des machines virtuelles Windows. Si vous utilisez CylanceOPTICS sur une machine virtuelle, BlackBerry recommande de désactiver le capteur de visibilité Advanced WMI en vue de réduire le nombre d'évènements enregistrés.

## Configuration requise : application CylancePROTECT Mobile

| Élément | Description |
|---|---|
| OS | Consultez la matrice de compatibilité Cylance Endpoint Security. |
| Navigateurs de terminal pris en charge | Dernière version de :<br>• Android : Google Chrome, Samsung Internet, Firefox, Brave<br>• iOS: Safari |
| Configuration du terminal | • Demandez aux utilisateurs d'activer JavaScript dans leur navigateur mobile par défaut. Cela est nécessaire pour activer l'application CylancePROTECT Mobile.<br>• Demandez aux utilisateurs Android d'autoriser l'activité en arrière-plan pour l'application CylancePROTECT Mobile après son installation. |

## Configuration requise : BlackBerry Connectivity Node

### Logiciel

| Élément | Description |
|---|---|
| Java Runtime Environment | JRE 17 (dernière version de mise à jour, 64 bits) |

### Matériel

| Composant | BlackBerry Connectivity Node |
|---|---|
| Processeur (CPU) | Six cœurs de processeur, E5-2670 (2,6 GHz), E5-2683 v4 (2,1 GHz) ou équivalent |
| Mémoire (RAM) | 12 Go |
| Espace disque (disque dur) | 64 Go |

#### Exigences supplémentaires de BlackBerry Connectivity Node

- Choisissez un compte d'annuaire disposant des autorisations de lecture pour chaque connexion à l'annuaire configurée que BlackBerry Connectivity Node peut utiliser pour accéder aux annuaires d'entreprise.
- Utilisez un compte Windows disposant des autorisations nécessaires pour installer et configurer le logiciel sur l'ordinateur qui hébergera BlackBerry Connectivity Node.
- Vérifiez que les ports sortants suivants sont ouverts dans le pare-feu de votre organisation afin que les composants BlackBerry Connectivity Node puissent communiquer avec BlackBerry Infrastructure (<*region*>.bbsecure.com, par exemple ca.bbsecure.com) :
  - 443 (HTTPS) pour activer BlackBerry Connectivity Node
  - 3101 (TCP) pour toute autre connexion sortante
- Installez le logiciel sur une version de Windows Server prise en charge par Microsoft.
- Vous pouvez installer BlackBerry Connectivity Node sur l'implémentation anglaise, française, espagnole, japonaise ou allemande du système d'exploitation.

# Configuration requise : connecteur CylanceGATEWAY

#### Matériel

| Composant | CylanceGATEWAY Connector |
|---|---|
| Processeur (CPU) | Deux cœurs de processeur |
| Mémoire (RAM) | 5 GB |
| Espace disque (disque dur) | 2 Go |

#### AWS

| Élément | Description |
|---|---|
| Type d'instance | BlackBerry recommande un type d'instance c6in ou c5n pour les environnements de production. |

# Configuration requise : agents CylanceGATEWAY

Si vous avez activé la fonctionnalité CylanceGATEWAY pour vos utilisateurs mobiles, ceux-ci peuvent activer le mode de travail à partir de l'application CylancePROTECT Mobile. Pour plus d'informations sur la configuration requise de CylancePROTECT Mobile, consultez Configuration requise : application CylancePROTECT Mobile.

| Élément | Configuration requise |
|---|---|
| Processeur (CPU) | • Prend en charge tous les terminaux Apple, y compris les terminaux Apple Silicon via Rosetta 2<br>• Prend en charge tous les processeurs x64<br>• Ne prend pas en charge les systèmes d'exploitation 32 bits<br>• Ne prend pas en charge les terminaux ARM |
| OS | Pour plus d'informations sur les systèmes d'exploitation pris en charge par l'agent CylanceGATEWAY, reportez-vous à la Matrice de compatibilité Cylance Endpoint Security. Pour connaitre les délais de prise en charge de tous les produits BlackBerry, consultez le Guide de référence du cycle de vie des logiciels BlackBerry Enterprise. |

# Configuration requise : CylanceAVERT

| Élément | Description |
|---|---|
| Agent CylanceAVERT | CylanceAVERT est un programme d'installation groupé qui inclut CylanceAVERT Microsoft Outlook le plug-in et les extensions de navigateur pour Chrome, Firefox et Microsoft Edge. |
| Agent CylancePROTECT Desktop | Agent CylancePROTECT Desktop version 3.1 ou versions ultérieures. |
| Prise en charge du système d'exploitation et de Microsoft Outlook | Pour plus d'informations sur la compatibilité des systèmes d'exploitation et des versions de Microsoft Outlook avec CylanceOPTICS, consultez Matrice de compatibilité Cylance Endpoint Security. Pour connaitre les délais de prise en charge de tous les produits BlackBerry, consultez le Guide de référence du cycle de vie des logiciels BlackBerry Enterprise. |
| .NET | • Microsoft .NET 4.6.2 ou versions ultérieures<br>• .NET Standard 2.0 ou une version ultérieure |
| Microsoft Visual C++ | Package redistribuable Microsoft Visual C++ 2017 ou version ultérieure |

# Configuration réseau requise pour Cylance Endpoint Security

#### Agents Cylance Endpoint Security

Le port 443 (HTTPS) doit être ouvert pour que les agents Cylance Endpoint Security Desktop puissent communiquer avec la console de gestion.

Les agents communiquent via des Websockets sécurisés (WSS) et doivent être en mesure d'établir cette connexion directement. Configurez le réseau de votre organisation pour autoriser les connexions aux domaines suivants.

**Remarque :**

- La console de gestion est hébergée par AWS et n'a pas d'adresses IP fixes. Vous pouvez autoriser le trafic HTTPS vers *.cylance.com. Pour l'hôte cylance-optics-files-use1.s3.amazonaws.com (et les hôtes similaires pour les autres régions), il est recommandé d'autoriser cet hôte spécifique. Il n'est pas recommandé d'autoriser *.amazonaws.com car il peut ouvrir votre réseau à d'autres hôtes.
- Veuillez noter que le domaine api2.cylance.com est obsolète, mais reste ouvert pour prendre en charge les agents CylancePROTECT Desktop plus anciens. api2.cylance.com dirige vers la même destination que api.cylance.com à des fins d'analyse des menaces et d'évaluation des risques.

| Élément | Description |
|---|---|
| Amérique du Nord | Requis pour la connexion à la console Cylance :<br>• login.cylance.com<br>• idp.blackberry.com<br>• cdn.cylance.com<br>• idp.cs.cylance.com |
| | Requis pour CylancePROTECT Desktop :<br>• data.cylance.com<br>• protect.cylance.com<br>• update.cylance.com<br>• api.cylance.com<br>• download.cylance.com<br>• venueapi.cylance.com |
| | Requis pour CylanceOPTICS :<br>• cylance-optics-files-use1.s3.amazonaws.com<br>• opticspolicy.cylance.com<br>• content.cylance.com<br>• rrws-use1.cylance.com<br>• collector.cylance.com<br>• scalar-api-use1.cylance.com<br>• cement.cylance.com |
| | Requis pour l'agent CylanceGATEWAY :<br>• idp.blackberry.com<br>• quip.webapps.blackberry.com<br>• us1.cs.blackberry.com<br>Requis pour CylanceGATEWAY Connector : deb.nodesource.com<br>Requis pour l'agent CylanceGATEWAY et CylanceGATEWAY Connector : us1.bg.blackberry.com<br>Pour plus d'informations, reportez-vous à KB79017. |

| Élément | Description |
| --- | --- |
| Asie-Pacifique Nord-est | Requis pour la connexion à la console Cylance :<br>• login-apne1.cylance.com<br>• idp.blackberry.com<br>• cdn.cylance.com<br>• idp.cs.cylance.com |
| | Requis pour CylancePROTECT Desktop :<br>• data-apne1.cylance.com<br>• protect-apne1.cylance.com<br>• update-apne1.cylance.com<br>• api.cylance.com<br>• download.cylance.com<br>• venueapi-apne1.cylance.com |
| | Requis pour CylanceOPTICS :<br>• cylance-optics-files-apne1.s3.amazonaws.com<br>• opticspolicy-apne1.cylance.com<br>• content-apne1.cylance.com<br>• rrws-apne1.cylance.com<br>• collector-apne1.cylance.com<br>• scalar-api-apne1.cylance.com<br>• cement-apne1.cylance.com |
| | Requis pour l'agent CylanceGATEWAY :<br>• idp.blackberry.com<br>• quip.webapps.blackberry.com<br>• jp1.cs.blackberry.com<br>Requis pour CylanceGATEWAY Connector : deb.nodesource.com<br>Requis pour l'agent CylanceGATEWAY et CylanceGATEWAY Connector : jp1.bg.blackberry.com<br>Pour plus d'informations, reportez-vous à KB79017. |
| Asie-Pacifique Sud-est | Requis pour la connexion à la console Cylance :<br>• login-au.cylance.com<br>• idp.blackberry.com<br>• cdn.cylance.com<br>• idp.cs.cylance.com |

| Élément | Description |
| --- | --- |
| | Requis pour CylancePROTECT Desktop :<br>• data-au.cylance.com<br>• protect-au.cylance.com<br>• update-au.cylance.com<br>• api.cylance.com<br>• download.cylance.com<br>• venueapi-au.cylance.com |
| | Requis pour CylanceOPTICS :<br>• cylance-optics-files-apse2.s3.amazonaws.com<br>• opticspolicy-au.cylance.com<br>• content-apse2.cylance.com<br>• rrws-apse2.cylance.com<br>• collector-apse2.cylance.com<br>• scalar-api-apse2.cylance.com<br>• cement-au.cylance.com<br>• cement-apse2.cylance.com |
| | Requis pour l'agent CylanceGATEWAY :<br>• idp.blackberry.com<br>• quip.webapps.blackberry.com<br>• au1.cs.blackberry.com<br>Requis pour CylanceGATEWAY Connector : deb.nodesource.com<br>Requis pour l'agent CylanceGATEWAY et CylanceGATEWAY Connector : au1.bg.blackberry.com<br>Pour plus d'informations, reportez-vous à KB79017. |
| Europe centrale | Requis pour la connexion à la console Cylance :<br>• login-euc1.cylance.com<br>• idp.blackberry.com<br>• cdn.cylance.com<br>• idp.cs.cylance.com |
| | Requis pour CylancePROTECT Desktop :<br>• data-euc1.cylance.com<br>• protect-euc1.cylance.com<br>• update-euc1.cylance.com<br>• api.cylance.com<br>• download.cylance.com<br>• venueapi-euc1.cylance.com |

| Élément | Description |
| --- | --- |
| | Requis pour CylanceOPTICS :<br>• cylance-optics-files-euc1.s3.amazonaws.com<br>• opticspolicy-euc1.cylance.com<br>• content-euc1.cylance.com<br>• rrws-euc1.cylance.com<br>• collector-euc1.cylance.com<br>• scalar-api-euc1.cylance.com<br>• cement-euc1.cylance.com |
| | Requis pour l'agent CylanceGATEWAY :<br>• idp.blackberry.com<br>• quip.webapps.blackberry.com<br>• eu1.cs.blackberry.com<br>Requis pour CylanceGATEWAY Connector : deb.nodesource.com<br>Requis pour l'agent CylanceGATEWAY et CylanceGATEWAY Connector : eu1.bg.blackberry.com<br>Pour plus d'informations, reportez-vous à KB79017. |
| Amérique du Sud | Requis pour la connexion à la console Cylance :<br>• login-sae1.cylance.com<br>• idp.blackberry.com<br>• cdn.cylance.com<br>• idp.cs.cylance.com |
| | Requis pour CylancePROTECT Desktop :<br>• data-sae1.cylance.com<br>• protect-sae1.cylance.com<br>• update-sae1.cylance.com<br>• api.cylance.com<br>• download.cylance.com<br>• venueapi-sae1.cylance.com |
| | Requis pour CylanceOPTICS :<br>• cylance-optics-files-sae1.s3.amazonaws.com<br>• opticspolicy-sae1.cylance.com<br>• content-sae1.cylance.com<br>• rrws-sae1.cylance.com<br>• collector-sae1.cylance.com<br>• scalar-api-sae1.cylance.com<br>• cement-sae1.cylance.com |

| Élément | Description |
| --- | --- |
| | Requis pour l'agent CylanceGATEWAY :<br>• idp.blackberry.com<br>• quip.webapps.blackberry.com<br>• br1.cs.blackberry.com<br>Requis pour CylanceGATEWAY Connector : deb.nodesource.com<br>Requis pour l'agent CylanceGATEWAY et CylanceGATEWAY Connector : br1.bg.blackberry.com<br>Pour plus d'informations, reportez-vous à KB79017. |
| GovCloud | Requis pour la connexion à la console Cylance :<br>• login.us.cylance.com<br>• idp.blackberry.com<br>• idp.cs.cylance.com |
| | Requis pour CylancePROTECT Desktop :<br>• data.us.cylance.com<br>• protect.us.cylance.com<br>• update.us.cylance.com<br>• api.us.cylance.com<br>• download.cylance.com<br>• download.us.cylance.com<br>• venueapi.us.cylance.com |
| | Requis pour CylanceOPTICS :<br>• cylance-optics-files.us.s3.amazonaws.com<br>• opticspolicy.us.cylance.com<br>• rrws.us.cylance.com<br>• collector.us.cylance.com<br>• scalar-api.us.cylance.com<br>• cement.us.cylance.com |

**Application CylancePROTECT Mobile**

L'application CylancePROTECT Mobile nécessite une connexion directe et sécurisée aux URL suivantes pour communiquer avec les services cloud CylancePROTECT Mobile. Si les terminaux sont connectés au réseau Wi-Fi de votre organisation, votre configuration réseau doit autoriser les connexions à :

- Services Cloud CylancePROTECT Mobile :
  - É-U : https://us1.mtd.blackberry.com
  - JP : https://jp1.mtd.blackberry.com
  - UE : https://eu1.mtd.blackberry.com
  - AU : https://au1.mtd.blackberry.com
  - SP : https://br1.mtd.blackberry.com
- Services communs Gateway :

  - É-U : https://us1.cs.blackberry.com
  - JP : https://jp1.cs.blackberry.com
  - UE : https://eu1.cs.blackberry.com
  - AU : https://au1.cs.blackberry.com
  - SP : https://br1.cs.blackberry.com
- https://score.cylance.com
- https://idp.blackberry.com
- https://mobile.ues.blackberry.com

# Conditions requises pour le proxy Cylance Endpoint Security

#### Configuration d'un proxy pour les agents CylancePROTECT Desktop et CylanceOPTICS

- Si vous souhaitez configurer à la fois l'agent CylancePROTECT Desktop et l'agent CylanceOPTICS sur un terminal pour utiliser un serveur proxy pour la communication sortante vers les serveurs BlackBerry, dans l'Éditeur de Registre, accédez à HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop et créez la valeur de chaîne REG_SZ :
  - Nom de la valeur = ProxyServer
  - Données de valeur = *<proxyIP:port>* (par exemple, http://123.45.67.89:8080)
- Le proxy doit accepter les demandes non autorisées. L'inspection SSL n'est pas prise en charge et doit être contournée pour tout le trafic de l'agent (*.cylance.com).

#### Options de proxy pour l'agent CylanceOPTICS

- L'agent CylanceOPTICS est compatible avec le proxy et interroge .NET Framework pour identifier et utiliser les paramètres de proxy disponibles. Si vous avez configuré la valeur ProxyServer dans le registre, l'agent CylanceOPTICS utilise le proxy spécifié. L'agent CylanceOPTICS essaie d'abord de communiquer en tant que système local, puis en tant qu'utilisateur actuellement connecté.
- Si vous configurez l'agent CylanceOPTICS pour qu'il utilise un proxy et qu'il ne peut pas communiquer avec les services cloud, l'agent tente de contourner le proxy pour établir une connexion directe. Sur les terminaux Windows et macOS, vous pouvez désactiver ce contournement de proxy. Procédez comme suit avant d'installer l'agent CylanceOPTICS :

| Plateforme | Étapes |
|---|---|
| Windows | Dans HKLM\SOFTWARE\Cylance\Optics\, créez une valeur de chaîne REG_SZ :<br>• Nom de la valeur = DisableProxyBypass<br>• Données de valeur = True |
| macOS | • Dans /Library/Application Support/Cylance/Desktop/registry/LocalMachine/Software/Cylance/Desktop/, ajoutez les éléments suivants au fichier values.xml :<br>`<value name="ProxyServer" type="string">http://proxy_server_IP:port</value>`<br>• Dans /Library/Application Support/Cylance/Optics/Configuration, créez un fichier ExternalConfig.xml avec les éléments suivants :<br>`<?xml version="1.0" encoding="utf-8"?><EnforceProxyServer>true</EnforceProxyServer>` |

- Lorsque CylanceOPTICS crée un évènement de détection impliquant un fichier signé en tant qu'artefact, il utilise une commande de l'API Windows pour valider la signature ou le certificat. La commande envoie une demande de validation à un serveur OCSP. L'adresse du serveur OCSP est déterminée par Windows. Si votre serveur proxy signale des tentatives d'envoi de trafic externe à un serveur OCSP, mettez à jour les paramètres de proxy sur les terminaux de façon à autoriser les connexions avec le serveur OCSP.

#### Linux : configurer les agents CylancePROTECT Desktop et CylanceOPTICS pour qu'ils utilisent un serveur proxy

Sur les versions prises en charge de RHEL, CentOS, Ubuntu, Amazon, Linux 2 et SUSE 15, utilisez les commandes suivantes pour configurer les agents afin qu'ils utilisent un proxy non authentifié ou authentifié. Vous pouvez utiliser ces commandes avant d'installer les agents. Les commandes ci-dessous configurent un proxy pour l'agent CylancePROTECT Desktop. Pour définir un proxy pour l'agent CylanceOPTICS :

- Remplacer toutes les instances de « cylancesvc » par « cyoptics »
- Dupliquez chaque ligne http_proxy et remplacez « http_proxy » par « https_proxy ». Dans la plupart des cas, https_proxy utilise la même valeur que http_proxy car le trafic HTTPS est tunnellisé à l'aide de TCP Connect, mais si votre organisation utilise un serveur proxy de terminaison HTTPS, spécifiez la valeur appropriée pour https_proxy.

**Proxy non authentifié :**

```
mkdir /etc/systemd/system/cylancesvc.service.d
echo "[Service]" > /etc/systemd/system/cylancesvc.service.d/proxy.conf
echo "Environment=http_proxy=http://proxyaddress:port" >> /etc/systemd/system/
cylancesvc.service.d/proxy.conf
systemctl stop cylancesvc
systemctl daemon-reload
systemctl start cylancesvc
```

**Proxy authentifié :**

```
mkdir /etc/systemd/system/cylancesvc.service.d
echo "[Service]" > /etc/systemd/system/cylancesvc.service.d/proxy.conf
echo "Environment=http_proxy=user:password@proxyaddress:port" >> /etc/systemd/
system/cylancesvc.service.d/proxy.conf
systemctl stop cylancesvc
systemctl daemon-reload
systemctl start cylancesvc
```

# Connexion à la console de gestion

Une fois votre compte activé, vous recevrez un e-mail contenant vos informations de connexion à la console de gestion Cylance Endpoint Security. Cliquez sur le lien dans l'e-mail pour ouvrir la page de connexion ou rendez-vous sur :

- **Amérique du Nord :** https://login.cylance.com
- **Asie-Pacifique Nord-Est :** https://login-apne1.cylance.com
- **Asie-Pacifique Sud-Est :** https://login-au.cylance.com
- **Europe centrale :** https://login-euc1.cylance.com
- **Amérique du Sud Est :** https://login-sae1.cylance.com
- **GovCloud :** https://login.us.cylance.com

L'adresse électronique servira d'informations de connexion à votre compte. Après avoir créé un mot de passe, vous pouvez accéder à la console.

**Exigences en matière de mot de passe**

Votre mot de passe doit comporter trois des caractères suivants :

- Un caractère en minuscule
- Un caractère en majuscule
- Un caractère spécial (par exemple, * # $ %).
- Un caractère numérique
- Données/Caractères Unicode (par exemple, ♥✹☆ )

**Délai d'expiration de la session**

La session s'éteint 1 heure après la dernière authentification réussie.

# Authentification personnalisée

**Important :** L'authentification personnalisée a été dépréciée et sera bientôt supprimée. Si vous utilisez l'authentification personnalisée pour accéder à Cylance Endpoint Security, vous pouvez migrer votre IDP externe vers un authentificateur et utiliser l'authentification améliorée pour accéder à la console Cylance. Pour en savoir plus sur l'authentification améliorée, consultez la section Authentification améliorée pour la connexion. Pour obtenir des instructions détaillées sur la configuration de votre IDP externe en tant qu'authentificateur, consultez la section Migrer des IDP externes de l'authentification personnalisée héritée vers la structure d'authentification moderne.

Utilisez des fournisseurs d'identité externes (IdP) pour vous connecter à la console de gestion. Pour ce faire, vous devez configurer les paramètres avec votre IdP afin d'obtenir un certificat X.509 et une URL pour vérifier votre connexion IdP. L'authentification personnalisée fonctionne avec Microsoft SAML 2.0. La compatibilité de cette fonctionnalité avec OneLogin, Okta, Microsoft Azure et PingOne a été confirmée. Cette fonctionnalité fournit également un paramètre personnalisé et doit fonctionner avec d'autres IdP qui suivent Microsoft SAML 2.0.

Pour obtenir des exemples d'utilisation de l'authentification personnalisée, reportez-vous aux articles suivants.

- Microsoft Azure
- Okta
- OneLogin
- PingOne
- Utilisation de SAML 2.0

**Remarque :** L'authentification personnalisée ne prend pas en charge les services ADFS (Active Directory Federation Services).

### Configurer l'authentification personnalisée

1. Dans la console de gestion, cliquez sur **Paramètres > Application** dans le menu.
2. Cochez la case **Authentification personnalisée**. Les options de configuration s'affichent.
3. Sélectionnez les options que vous souhaitez utiliser pour l'authentification. Reportez-vous à la section Descriptions de l'authentification personnalisée pour obtenir une description des options.
4. Cliquez sur **Enregistrer**.

### Descriptions de l'authentification personnalisée

| Option | Description |
|---|---|
| Strong Authentication | Sélectionnez cette option pour fournir un accès à authentification multifacteur. |
| Identification unique | Sélectionnez cette option pour fournir un accès à authentification unique (SSO).<br>Si vous sélectionnez Strong Authentication ou SSO, les paramètres d'authentification personnalisée ne sont pas affectés, car tous les paramètres de configuration sont gérés par le fournisseur d'identité (IdP). |
| Autoriser la connexion par mot de passe | Cette option vous permet de vous connecter directement à la console à l'aide de l'authentification unique (SSO). Cela vous permet de tester vos paramètres SSO sans être verrouillé sur la console. Une fois que vous êtes connecté à la console à l'aide de SSO, il est recommandé de désactiver cette fonction. |
| Fournisseur | Sélectionnez le fournisseur de services pour l'authentification personnalisée. |
| Certificat X.509 | Saisissez les informations de certification X.509. |
| URL de connexion | Saisissez l'URL de l'authentification personnalisée. |

### Migration des IDP externes de l'authentification personnalisée vers un authentificateur

Lorsque vous vous connectez à la console de gestion à l'aide d'un fournisseur d'identité externe (IDP) configuré pour l'authentification personnalisée, vous devez vous connecter à l'aide du lien « Ou connectez-vous avec votre fournisseur d'identité externe » avec vos informations d'identification IDP externes. BlackBerry recommande de configurer votre IDP externe en tant qu'authentificateur et d'utiliser une stratégie d'authentification pour vous connecter à partir de l'écran de connexion principal à l'aide de vos informations d'identification IDP. La configuration de votre IDP externe en tant qu'authentificateur permet d'obtenir plus de granularité et de flexibilité dans la configuration de l'authentification.

Pour configurer un IDP externe afin qu'il se connecte à la console de gestion à partir de l'écran principal de connexion, procédez comme suit. Pour plus d'informations, consultez la section Migrer des IDP externes de l'authentification personnalisée vers un authentificateur.

Si vous avez configuré votre IdP existant en tant qu'authentificateur avant décembre 2023 et que vous souhaitez autoriser les utilisateurs à accéder directement à la console Cylance à partir du portail utilisateur IdP, reportez-vous à la section Authentification améliorée pour la connexion.

| Étape | Action |
| --- | --- |
| 1 | Examinez Considérations relatives à l'ajout d'authentificateurs SAML. |
| 2 | Connectez-vous à la console Cylance avec votre IDP externe. |
| 3 | Configurez l'IDP externe pour communiquer avec Cylance Endpoint Security.<br>• Enregistrez les informations d'authentification personnalisées<br>• Configurez l'authenticateur |
| 4 | Gérer les stratégies d'authentification pour votre locataire qui utilise l'authentificateur que vous avez créé.<br>**Remarque :** En tant que sécurité intégrée, créez une stratégie utilisateur qui utilise uniquement le mot de passe de la console Cylance et attribuez-la à un administrateur. |
| 5 | Vérifiez que la case Autoriser la connexion par mot de passe (Paramètres > Application > Authentification personnalisée) est cochée. Cette option vous permet de vous connecter directement à la console à l'aide de l'authentification unique (SSO). Cette option permet de tester vos paramètres SSO sans être verrouillé sur la console. |
| 6 | Connectez-vous à la console Cylance à partir de l'écran principal de connexion et testez la stratégie d'informations d'identification de connexion IDP externe. |
| 7 | (Facultatif) Désactivez l'authentification personnalisée (Paramètres > Application). |

# Authentification améliorée pour la connexion

La console de gestion fournit des fonctions d'authentification améliorées, notamment l'authentification à plusieurs facteurs locale et des affectations de stratégies et des stratégies d'authentification plus granulaires. Vous pouvez configurer l'environnement pour spécifier les types d'authentification que les administrateurs doivent effectuer lorsqu'ils se connectent à la console Cylance et que les utilisateurs doivent réaliser lorsqu'ils activent des agents ou des applications Cylance Endpoint Security. Par défaut, les administrateurs utilisent le mot de passe de la console Cylance pour accéder à la console de gestion et aux utilisateurs pour activer les agents et les applications Cylance Endpoint Security. Pour les locataires créés en mars 2024 ou à une date ultérieure, par défaut, les administrateurs devront saisir un mot de passe à usage unique pour accéder à la console Cylance après avoir configuré leur mot de passe de console.

Vous pouvez créer des stratégies d'authentification pour votre locataire qui spécifient les types d'authentification qui doivent être effectués par tous les administrateurs et utilisateurs du locataire. Une seule stratégie de locataire peut être créée pour l'ouverture de session de la console Cylance, les applications Cylance Endpoint Security et les agents de bureau Cylance Endpoint Security. Vous pouvez créer des stratégies d'authentification pour les utilisateurs qui spécifient les types d'authentification que les administrateurs et les utilisateurs du locataire doivent effectuer. Le type d'authentification ajouté à la stratégie du locataire et à la stratégie d'authentification doit être effectué dans l'ordre dans lequel ils sont spécifiés dans la stratégie. En tant que sécurité intégrée, vous pouvez configurer un administrateur pour qu'il accède à la console Cylance à l'aide de son nom d'utilisateur et d'un mot de passe fort.

**Remarque :** Le flux de connexion mis à jour est désormais la seule méthode pour accéder à la console Cylance. Toutes les stratégies d'authentification que vous avez appliquées dans votre console au cours de la période d'aperçu ont pris effet.

Pour configurer une authentification améliorée pour la connexion, effectuez l'une des opérations suivantes :

#### Configurer l'authentification améliorée pour la connexion à la console Cylance

Si votre locataire a été créé avant mars 2024, procédez comme suit si vous souhaitez configurer vos utilisateurs pour qu'ils s'authentifient auprès de la console Cylance à l'aide d'un authentificateur tel qu'un mot de passe à usage unique en plus du mot de passe Cylance. Pour savoir comment ajouter l'authentificateur par mot de passe à usage unique à votre stratégie de locataire, reportez-vous à la section Ajouter l'authentification par mot de passe à usage unique pour permettre aux administrateurs d'accéder à la console Cylance.

| Étape | Action |
|---|---|
| 1 | Connectez-vous à la console Cylance à l'aide de votre nom d'utilisateur et de votre mot de passe existants. |
| 2 | Ajoutez un authentificateur (par exemple, Mot de passe à usage unique ou Enterprise). Par défaut, les authentificateurs suivants sont configurés pour être utilisés dans votre environnement : mot de passe à usage unique, mot de passe de console Cylance et authentification Enterprise. |
| 3 | Créez une stratégie d'authentification qui utilise le mot de passe et l'authentificateur que vous avez créés (facultatif).<br>**Remarque :** En tant que sécurité intégrée, créez une stratégie d'authentification qui utilise uniquement le mot de passe de la console Cylance et attribuez-la à un administrateur. |
| 4 | Créez une stratégie de locataire pour les administrateurs et les utilisateurs. |

#### Supprimer l'authentification par mot de passe à usage unique pour vous connecter à la console Cylance

Les locataires créés en mars 2024 ou à une date ultérieure exigent que les utilisateurs saisissent un mot de passe à usage unique après chaque saisie du mot de passe de la console Cylance avant de pouvoir accéder à la console. Procédez comme suit si vous souhaitez supprimer le mot de passe à usage unique requis pour que les utilisateurs s'authentifient auprès de la console. Pour savoir comment supprimer l'authentificateur par mot de passe à usage unique de votre stratégie de locataire, reportez-vous à la section Supprimer l'authentification par mot de passe à usage unique pour permettre aux administrateurs d'accéder à la console Cylance.

| Étape | Action |
|---|---|
| 1 | Connectez-vous à la console Cylance à l'aide de votre nom d'utilisateur et de votre mot de passe à usage unique existants. |
| 2 | Supprimez l'authentificateur de mot de passe à usage unique de la stratégie de locataire de la console d'administration. |

| Étape | Action |
|---|---|
| 3 | Connectez-vous à la console Cylance et testez la stratégie de mot de passe de la console Cylance. |

#### Configurer un nouvel authentificateur IDP SAML pour l'authentification SSO et l'accès initié par IDP à la console Cylance

Procédez comme suit si vous souhaitez configurer un nouvel authentificateur IDP SAML pour que les utilisateurs s'authentifient auprès de la console Cylance. Les utilisateurs peuvent utiliser leurs informations d'identification IDP pour accéder à la console à partir de la page d'ouverture de session ou utiliser l'authentification SSO initiée par IDP pour accéder à la console à partir du portail utilisateur IDP. Pour savoir comment configurer votre IDP SAML, reportez-vous à la section Comment configurer des IDP SAML pour une authentification améliorée et un accès initié par IDP à la console Cylance, puis sélectionnez votre IDP.

| Étape | Action |
|---|---|
| 1 | Dans l'environnement IDP, créez une nouvelle application SAML. |
| 2 | Configurez l'IDP pour communiquer avec Cylance Endpoint Security. |
| 3 | Dans la console Cylance, ajoutez un authentificateur. |
| 4 | Créez une stratégie d'authentification qui utilise le mot de passe et l'authentificateur que vous avez créés.<br>**Remarque :** En tant que sécurité intégrée, créez une stratégie d'authentification qui utilise uniquement le mot de passe de la console Cylance et attribuez-la à un administrateur. |
| 5 | Dans l'environnement IDP, mettez à jour l'URL de rappel SSO que vous avez générée dans la console Cylance. |
| 6 | Connectez-vous à la console Cylance à partir de l'écran principal de connexion et testez la stratégie d'informations d'identification de connexion IDP externe. |
| 7 | (Facultatif) Désactivez l'authentification personnalisée (Paramètres > Application). |

#### Mettre à jour un authentificateur IDP SAML existant pour activer l'accès initié par IDP à la console Cylance

Suivez ces étapes uniquement si votre authentificateur IDP SAML a été créé avant décembre 2023 et si vous souhaitez activer l'authentification SSO initiée par IDP pour que les utilisateurs puissent accéder à la console à partir du portail utilisateur IDP. Pour obtenir des instructions détaillées, reportez-vous à la section Comment mettre à jour les authentificateurs IDP (SAML) pour activer l'accès initié par IDP à la console Cylance et sélectionnez votre IDP.

| Étape | Action |
|---|---|
| 1 | Connectez-vous à la console Cylance à l'aide de votre nom d'utilisateur et de votre mot de passe existants. |
| 2 | Dans l'authentificateur IDP SAML actuel, générez une nouvelle URL de rappel SSO. |
| 3 | Mettez à jour la stratégie d'authentification actuelle avec l'URL de rappel SSO que vous venez de générer. |
| 4 | Dans l'environnement IDP, mettez à jour les paramètres SAML existants. |

### Se connecter à la console de gestion Cylance Endpoint Security à l'aide de l'authentification améliorée

Vous pouvez configurer des stratégies d'authentification qui spécifient les types d'authentification que les administrateurs doivent effectuer pour se connecter à la console de gestion Cylance Endpoint Security et que les utilisateurs doivent effectuer pour activer des agents ou des applications Cylance Endpoint Security (par exemple, l'application CylancePROTECT Mobile et l'agent CylanceGATEWAY). Un écran de transition s'affiche brièvement avant l'accès à la console de gestion Cylance Endpoint Security.

Si vous vous connectez à l'aide d'un IDP externe configuré pour l'authentification personnalisée dans la console de gestion (Paramètres > Authentification personnalisée), vous devez continuer à vous connecter à l'aide du lien « Ou connectez-vous avec votre fournisseur d'identité externe » avec vos informations d'identification IDP tierces externes. BlackBerry recommande de configurer votre IDP externe en tant qu'authentificateur afin de pouvoir utiliser une stratégie d'authentification pour vous connecter avec vos informations d'identification IDP tierces à partir de l'écran de connexion principal. Cela offre davantage de granularité et de flexibilité dans la configuration de l'authentification. Pour plus d'informations sur la configuration de votre adresse IDP externe en tant qu'authentificateur, consultez Migration des IDP externes de l'authentification personnalisée vers un authentificateur.

Si vous avez configuré votre IdP externe en tant qu'authentificateur avant décembre 2023, les utilisateurs ne pourront pas accéder à la console Cylance directement depuis le portail utilisateur de leur IdP externe à l'aide de l'authentification unique. Pour activer cette fonction, vous devez générer une nouvelle demande de connexion avec authentification unique Cylance Endpoint Security. Pour plus d'informations sur l'activation de la connexion initiée par un IdP sur la console Cylance, reportez-vous aux sections Authentification améliorée pour la connexion et Comment mettre à jour l'IdP externe pour activer l'accès SSO à la console Cylance.

**Avant de commencer :** Créez une stratégie d'authentification et attribuez-la aux administrateurs, aux utilisateurs et aux groupes dont les administrateurs et les utilisateurs font partie.

Effectuez l'une des tâches suivantes pour accéder à la console de gestion.

| Accès | Tâche | Étapes |
|---|---|---|
| Écran principal de connexion Cylance Endpoint Security. | Connectez-vous avec votre compte Cylance. | **a.** Entrez votre adresse e-mail.<br>**b.** Cliquez sur **Connexion**.<br>**c.** Saisissez votre mot de passe.<br>**d.** Cliquez sur **Connexion**. |

| Accès | Tâche | Étapes |
|---|---|---|
| | Connectez-vous à votre fournisseur d'identité externe configuré en tant qu'authentificateur. | **a.** Entrez votre adresse e-mail.<br>**b.** Cliquez sur **Connexion**.<br>**c.** Saisissez votre mot de passe.<br>**d.** Cliquez sur **Connexion**. |
| | Connectez-vous à votre fournisseur d'identité externe. | **a.** Cliquez sur **Ou connectez-vous à votre fournisseur d'identité externe**.<br>**b.** Dans le navigateur, saisissez votre adresse e-mail.<br>**c.** Cliquez sur **Connexion**.<br>**d.** Saisissez votre mot de passe<br>**e.** Cliquez sur **Connexion**. |
| Portail des utilisateurs d'IdP externe | Utilisez l'authentification unique pour vous connecter à l'aide des informations d'identification de votre fournisseur d'identité externe. | **a.** Connectez-vous au portail utilisateur de votre IdP.<br>**b.** Cliquez sur l'application qui vous est attribuée. |

### Générer une nouvelle URL de rappel SSO

Vous pouvez utiliser l'option Copier pour copier vos informations d'authentification actuelles et créer la nouvelle URL de rappel SSO. L'option Copier supprime l'URL de rappel SSO actuelle et en génère une nouvelle lorsque l'authentificateur copié est enregistré.

**Important** : effectuez cette tâche uniquement si vous avez configuré votre environnement pour une connexion améliorée, que votre authentificateur a été créé avant décembre 2023 et que vous souhaitez activer l'authentification unique (SSO) initiée par IdP sur la console. Pour vérifier si l'authentificateur a été créé avant décembre 2023, dans la console Cylance, ouvrez l'authentificateur SAML de l'IdP (Paramètres > Authentification).

- Si l'URL de rappel SSO est au format https://login.eid.blackberry.com/_/resume/saml20/<*hash*>, aucune autre action n'est requise.
- Si l'URL de rappel SSO est https://idp.blackberry.com/_/resume, procédez comme suit pour générer l'URL mise à jour.

**Avant de commencer :** L'authentificateur SAML de l'IdP a été créé avant décembre 2023 et utilise l'URL de rappel SSO obsolète.

1. Ouvrez l'écran Authentificateurs (Paramètres > Authentification).
2. Cliquez sur l'authentificateur SAML de l'IDP actuel.
3. Cliquez sur l'icône Copier dans le coin supérieur droit de l'écran.
4. Mettez à jour le nom de l'authentificateur copié. Cliquez sur **Enregistrer**.
5. Indiquez l'authentificateur que vous avez copié. Enregistrez l'**URL de rappel SSO**.
6. Supprimez l'authentificateur de l'IDP précédent.

**À la fin :** Mettez à jour la stratégie d'authentification actuelle avec l'authentificateur copié.

# Configuration d'un nouveau locataire Cylance Endpoint Security

Lorsque vous créez un nouveau locataire Cylance Endpoint Security, ou lorsque vous réinitialisez un locataire à l'état par défaut recommandé, le locataire inclut des zones préconfigurées et des stratégies de terminal préconfigurées conçues pour vous aider à adapter votre environnement à la posture de sécurité souhaitée.

Un nouveau locataire, ou un locataire qui a été réinitialisé à l'état par défaut recommandé, comprend trois zones préconfigurées, une pour chaque système d'exploitation de poste de travail (Windows, macOS et Linux). Ces zones sont configurées pour attribuer automatiquement de nouveaux terminaux de bureau à la zone de système d'exploitation appropriée. La stratégie de terminal de phase 1 décrite ci-dessous est attribuée aux zones préconfigurées.

Un nouveau locataire ou un locataire réinitialisé inclut trois stratégies de terminal préconfigurées pour contrôler les fonctionnalités de CylancePROTECT Desktop et de CylanceOPTICS. Reportez-vous à la section Paramètres de configuration par défaut pour un nouveau locataire Cylance Endpoint Security pour connaître la configuration complète de chaque stratégie préconfigurée.

| Stratégie préconfigurée | Description |
|---|---|
| Étape 1 | La configuration de démarrage qui permet aux terminaux d'être à l'écoute des menaces de logiciels malveillants. Les paramètres de stratégie avancés sont désactivés. Utilisez d'abord cette stratégie dans votre environnement pour observer les détections initiales provenant des terminaux et pour configurer les exceptions appropriées.<br><br>Lorsque vous êtes à l'aise avec les performances et l'impact de cette stratégie, vous pouvez faire passer les terminaux à la stratégie d'étape 2. |
| Étape 2 | Cette stratégie de terminal permet de détecter un plus large éventail de menaces, y compris les logiciels malveillants anormaux, les scripts dangereux et les failles de mémoire. Attribuez cette stratégie à un petit nombre de terminaux pour évaluer le volume et la fréquence des détections, ainsi que le niveau d'investigation requis. Cela vous permettra d'affiner la configuration de la stratégie avant de l'attribuer à d'autres terminaux.<br><br>Lorsque vous êtes à l'aise avec les performances de cette stratégie, vous pouvez faire passer les terminaux à la stratégie d'étape 3. |
| Étape 3 | Cette stratégie de terminal s'appuie sur l'étape 2 en réglant les paramètres afin que les terminaux puissent à la fois détecter les menaces et prendre certaines mesures préventives. Utilisez cette stratégie de terminal uniquement après avoir suffisamment testé la stratégie de l'étape 2 et après avoir appliqué le réglage fin de la stratégie de l'étape 2 à cette stratégie. |

Au fur et à mesure que vous testez et évaluez les zones préconfigurées et les stratégies de terminal, vous pouvez ajuster la configuration selon vos besoins, notamment en apportant des modifications aux options préconfigurées ou en copiant et en modifiant une zone ou une stratégie pour déterminer la configuration la mieux adaptée à l'environnement de votre entreprise.

Cylance Endpoint Security propose également des options supplémentaires qui vous permettent de configurer rapidement un nouveau locataire en fonction des besoins de votre entreprise. Vous pouvez exporter la configuration d'un locataire et l'importer vers un nouveau locataire, ou réinitialiser un locataire aux paramètres par défaut recommandés comme détaillé dans Paramètres de configuration par défaut pour un nouveau

locataire Cylance Endpoint Security. Pour plus d'informations, reportez-vous à Exporter, importer ou réinitialiser la configuration d'un locataire Cylance Endpoint Security.

# Paramètres de configuration par défaut pour un nouveau locataire Cylance Endpoint Security

**Zones préconfigurées**

| Zones préconfigurées | Stratégie de terminal attribuée | Règles de zone par défaut |
|---|---|---|
| Zone Windows | Étape 1 | Attribution automatique de zone pour déplacer tous les nouveaux terminaux Windows dans cette zone. |
| Zone Mac | Étape 1 | Attribution automatique de zone pour déplacer tous les nouveaux terminaux macOS dans cette zone. |
| Zone Linux | Étape 1 | Attribution automatique de zone pour déplacer tous les nouveaux terminaux Linux dans cette zone. |

**Stratégies de terminal préconfigurées**

| Configuration de la stratégie de terminal | Stratégie d'étape 1 | Stratégie d'étape 2 | Stratégie d'étape 3 |
|---|---|---|---|
| **Actions de fichier** | | | |
| Mise en quarantaine automatique avec contrôle d'exécution : dangereuse | O | I | I |
| Mise en quarantaine automatique avec contrôle d'exécution : anormale | O | O | I |
| Activer la suppression automatique des fichiers mis en quarantaine | O | I | I |
| Transfert automatique : exécutable | I | I | I |
| **Actions de mémoire** | | | |
| Protection de la mémoire | O | I | I |
| Exploitation : pivot de pile | O | Ignorer | Ignorer |
| Exploitation : protection des piles | O | Ignorer | Ignorer |
| Exploitation : écraser le code | O | Ignorer | Ignorer |

| Configuration de la stratégie de terminal | Stratégie d'étape 1 | Stratégie d'étape 2 | Stratégie d'étape 3 |
|---|---|---|---|
| Exploitation : raclage de RAM | O | Alerte | Bloquer |
| Exploitation : charge utile malveillante | O | Ignorer | Ignorer |
| Exploitation : surveillance des appels système | O | Ignorer | Ignorer |
| Exploitation : appels système directs | O | Ignorer | Ignorer |
| Exploitation : écrasement de la DLL système | O | Ignorer | Ignorer |
| Exploitation : objet COM dangereux | O | Ignorer | Ignorer |
| Exploitation : injection via APC | O | Ignorer | Ignorer |
| Exploitation : macro VBA dangereuse | O | Ignorer | Ignorer |
| Injection de processus : allocation de mémoire à distance | O | Alerte | Bloquer |
| Injection de processus : mappage à distance de la mémoire | O | Alerte | Bloquer |
| Injection de processus : écriture à distance dans la mémoire | O | Alerte | Bloquer |
| Injection de processus : écriture à distance de PE dans la mémoire | O | Alerte | Bloquer |
| Injection de processus : code d'écrasement à distance | O | Ignorer | Ignorer |
| Injection de processus : démappage à distance de la mémoire | O | Ignorer | Ignorer |
| Injection de processus : création de thread à distance | O | Ignorer | Ignorer |
| Injection de processus : APC à distance programmé | O | Ignorer | Ignorer |
| Injection de processus : injection DYLD | O | Ignorer | Ignorer |
| Injection de processus : Doppelganger | O | Ignorer | Ignorer |
| Injection de processus : variable environnementale dangereuse | O | Ignorer | Ignorer |
| Escalade : lecture LSASS | O | Alerte | Bloquer |
| Escalade : aucune allocation | O | Alerte | Bloquer |

| Configuration de la stratégie de terminal | Stratégie d'étape 1 | Stratégie d'étape 2 | Stratégie d'étape 3 |
|---|---|---|---|
| Escalade : modifications des autorisations de mémoire dans d'autres processus | O | Ignorer | Ignorer |
| Escalade : modifications des autorisations de mémoire dans les processus enfants | O | Ignorer | Ignorer |
| Escalade : jeton système volé | O | Ignorer | Ignorer |
| Escalade : début du processus à faible intégrité | O | Ignorer | Ignorer |
| **Paramètres de protection** | | | |
| Empêcher l'arrêt du service à partir du terminal | I | I | I |
| Arrêter les processus en cours d'exécution dangereux et leurs sous-processus | O | O | O |
| Détection des menaces en arrière-plan | I | I | I |
| Réglage de l'exécution | Récurrent | Récurrent | Récurrent |
| Jours | 10 | 10 | 10 |
| Contrôler les nouveaux fichiers | I | I | I |
| Mo | 150 | 150 | 150 |
| Exclure des dossiers spécifiques | O | O | O |
| Copier les exemples de fichier | O | O | O |
| **Paramètres CylanceOPTICS** | | | |
| CylanceOPTICS | O | O | O |
| Activer les notifications de bureau CylanceOPTICS | O | O | O |
| Paramètres de détection | Aucun | Aucun | Aucun |
| **Contrôle d'applications** | | | |
| Contrôle d'applications | O | O | O |
| **Paramètres de l'agent** | | | |
| Activer le chargement automatique des fichiers journaux | O | O | O |
| Activer les notifications de bureau | O | O | O |

| Configuration de la stratégie de terminal | Stratégie d'étape 1 | Stratégie d'étape 2 | Stratégie d'étape 3 |
|---|---|---|---|
| Activer l'inventaire logiciel | I | I | I |
| **Contrôle de script** | | | |
| Contrôle de script | O | I | I |
| Script actif | O | Alerte | Blocage dangereux |
| Script PowerShell | O | Alerte | Blocage dangereux |
| Console PowerShell | O | Désactivé | Désactivé |
| Macros | O | Désactivé | Désactivé |
| Python | O | Désactivé | Désactivé |
| .NET DLR | O | Désactivé | Désactivé |
| Macros XLM | O | Désactivé | Désactivé |
| Avancé : noter tous les scripts | O | I | I |
| Avancé : télécharger le script sur le Cloud | O | I | I |
| Avancé : alerte uniquement en cas d'exécution de scripts suspects | O | I | I |
| **Contrôle du terminal** | | | |
| Contrôle du terminal Windows | I | I | I |
| Android | Accès complet | Accès complet | Accès complet |
| iOS | Accès complet | Accès complet | Accès complet |
| Image fixe | Accès complet | Accès complet | Accès complet |
| CD USB DVD RW | Accès complet | Accès complet | Accès complet |
| Clé USB | Accès complet | Accès complet | Accès complet |
| Relais USB VMware | Accès complet | Accès complet | Accès complet |
| Périphérique portable Windows | Accès complet | Accès complet | Accès complet |

# Exporter, importer ou réinitialiser la configuration d'un locataire Cylance Endpoint Security

Vous pouvez configurer un nouveau locataire Cylance Endpoint Security en exportant la configuration d'un locataire existant et en l'important dans le nouveau locataire. Vous avez également la possibilité de réinitialiser un nouveau locataire pour qu'il utilise les paramètres par défaut recommandés.

Les paramètres suivants sont inclus lorsque vous exportez la configuration d'un locataire existant et sont modifiés lorsque vous importez ou réinitialisez la configuration du locataire :

- Stratégies des terminaux
- Configurations de zone
- Paramètres de mise à jour de l'agent
- Listes mondiales sécurisées et de quarantaine
- Paramètres Syslog

**Remarque :** Les options d'exportation, d'importation et de réinitialisation sont spécialement conçues pour vous aider à configurer un nouveau locataire et à tester les paramètres avant d'inscrire des terminaux. La fonction d'exportation n'est pas destinée à être utilisée pour créer un fichier de configuration de sauvegarde pour un locataire existant. Lorsque vous importez une configuration vers un nouveau locataire ou que vous réinitialisez un locataire, la configuration précédente des éléments détaillés ci-dessus est supprimée et ne peut pas être restaurée.

1. Sur la barre de menus de la console de gestion, cliquez sur **Paramètres > Paramètres du locataire**.
2. Effectuez l'une des opérations suivantes :

| Tâche | Étapes |
|---|---|
| Exportez la configuration du locataire actuel. | Notez que seules les zones et les règles de zone qui ont été créées avec une requête enregistrée sont incluses dans la configuration exportée. Le fichier de configuration que vous exportez ne peut être importé que vers un nouveau locataire de la même région. Le fichier de configuration exporté n'est pas valide pour les locataires ayant une région différente.<br>**a.** Cliquez sur **Exporter**.<br>**b.** Attribuez un nom au fichier .zip.<br>**c.** Cliquez sur **Exporter**.<br>**d.** Reportez-vous aux instructions ci-dessous pour importer la configuration vers un nouveau locataire. |
| Importez les paramètres de configuration que vous avez exportés d'un autre locataire vers ce locataire. | Notez que l'importation de la configuration d'un locataire supprimera la configuration actuelle du locataire, y compris toute association entre les terminaux et les stratégies et zones de terminaux. Une fois supprimée, la configuration ne peut plus être restaurée.<br>**a.** Cliquez sur **Importer**.<br>**b.** Accédez au fichier de configuration .zip et sélectionnez-le.<br>**c.** Dans le champ de confirmation, saisissez **importer**.<br>**d.** Cliquez sur **Importer**.<br>**e.** Confirmez l'importation.<br>Si le processus échoue, toutes les modifications appliquées au locataire sont annulées. |

| Tâche | Étapes |
| --- | --- |
| Réinitialisez un locataire aux paramètres par défaut recommandés. | La réinitialisation de la configuration du locataire aux paramètres par défaut supprime la configuration actuelle, y compris toute association entre les terminaux et les stratégies et zones de terminaux. Une fois supprimée, la configuration ne peut plus être restaurée.<br>**a.** Cliquez sur **Réinitialiser**.<br>**b.** Dans le champ de confirmation, saisissez **réinitialiser**.<br>**c.** Cliquez sur **Réinitialiser**.<br>**d.** Confirmez la réinitialisation.<br>Si le processus échoue, toutes les modifications appliquées au locataire sont annulées. |

Les détails de l'importation ou de la réinitialisation sont consignés dans le journal d'audit.

# Installation de BlackBerry Connectivity Node

Le BlackBerry Connectivity Node vous permet de créer une connexion sécurisée entre Cylance Endpoint Security et un répertoire Microsoft Active Directory ou LDAP sur site. Cylance Endpoint Security peut synchroniser des terminaux, des utilisateurs et des groupes à partir de Active Directory. Les utilisateurs créés via la synchronisation de répertoire peuvent être activés pour l'application CylancePROTECT Mobile, CylanceGATEWAY et CylanceAVERT.

Vous pouvez installer une ou plusieurs instances de BlackBerry Connectivity Node pour assurer la redondance. Chaque instance doit être installée sur un ordinateur dédié. Si vous avez plusieurs BlackBerry Connectivity Node vous devez tous les mettre à niveau vers la même version logicielle. Après la mise à niveau de la première instance, les services d'annuaire sont désactivés jusqu'à ce que toutes les instances soient mises à niveau vers la même version.

Vous pouvez configurer une ou plusieurs connexions au répertoire, mais si vous avez plusieurs instances de BlackBerry Connectivity Node, toutes les connexions au répertoire doivent être configurées de manière identique dans chaque instance. Si une connexion au répertoire est manquante ou mal configurée, ce BlackBerry Connectivity Node apparaît comme désactivé dans la console de gestion.

Vous n'avez pas besoin d'installer BlackBerry Connectivity Node pour synchroniser avec Microsoft Entra ID Active Directory. Pour plus d'informations, reportez-vous à Configurer Cylance Endpoint Security pour la synchronisation avec EntraActive Directory.

Pour installer BlackBerry Connectivity Node, effectuez les opérations suivantes.

| Étape | Action |
|---|---|
| 1 | Consultez les exigences. |
| 2 | Définir une variable d'environnement pour l'emplacement Java. |
| 3 | Télécharger les fichiers d'installation et d'activation de BlackBerry Connectivity Node. |
| 4 | Installer et configurer BlackBerry Connectivity Node. |
| 5 | Si votre environnement a plusieurs instances de BlackBerry Connectivity Node, reportez-vous à Copier les configurations de connexion au répertoire. |
| 6 | Configurer des paramètres proxy pour une instance de BlackBerry Connectivity Node (Facultatif). |

## Définir une variable d'environnement pour l'emplacement Java

Vous devez installer une implémentation de JRE 17 sur les serveurs sur lesquels vous avez prévu d'installer BlackBerry Connectivity Node et une variable d'environnement doit pointer vers l'emplacement d'accueil Java.

Au début de l'installation, BlackBerry Connectivity Node vérifie qu'il peut trouver Java. Si Java est introuvable, l'application de configuration s'arrêtera dans le panneau de configuration requise et vous devrez définir une variable d'environnement pour l'emplacement Java et vous assurer que le dossier bin de Java est inclus dans la variable système Path. Notez que vous devrez fermer le programme d'installation à ce stade et le redémarrer uniquement après la création ou la mise à jour de la variable d'environnement.

**Avant de commencer :** Vérifiez que JRE 17 est installé sur le serveur sur lequel vous allez installer BlackBerry Connectivity Node.

1. Ouvrez la boite de dialogue **Paramètres système avancés Windows**.
2. Cliquez sur **Variables d'environnement**.
3. Dans la liste **Variables système**, cliquez sur **Nouveau**.
4. Dans le champ **Nom de variable**, saisissez `BB_JAVA_HOME`.
5. Dans le champ **Valeur de la variable**, saisissez le chemin d'accès au dossier JRE et cliquez sur **OK**.
6. Dans la liste **Variables système**, sélectionnez **Path** et cliquez sur **Modifier**.
7. Si le chemin n'inclut pas le dossier bin de Java, cliquez sur **Nouveau** et ajoutez `%BB_JAVA_HOME%\bin` au chemin.
8. Déplacez l'entrée %BB_JAVA_HOME%\bin suffisamment haut dans la liste pour qu'elle ne soit pas remplacée par une autre entrée, puis cliquez sur **OK**.

**À la fin :** Télécharger les fichiers d'installation et d'activation de BlackBerry Connectivity Node.

# Télécharger les fichiers d'installation et d'activation de BlackBerry Connectivity Node

**Avant de commencer :** Définir une variable d'environnement pour l'emplacement Java.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Connexions à l'annuaire**.
2. Cliquez sur l'onglet **Connectivity Node**.
3. Cliquez sur **Ajouter Connectivity Node**.
4. Sur la page de téléchargement logicielle, cliquez sur **Télécharger**.
5. Sélectionnez **BlackBerry Connectivity Node for UES**
6. Cliquez sur **Télécharger**.
7. Extrayez les fichiers d'installation de BlackBerry Connectivity Node sur l'ordinateur.

   Si vous installez plusieurs instances de BlackBerry Connectivity Node, ne copiez pas les fichiers d'installation utilisés entre les ordinateurs. Vous devez extraire les fichiers d'installation sur chaque ordinateur.
8. Dans la console de gestion, cliquez sur **Télécharger le fichier d'activation**.
9. Enregistrez le fichier d'activation (.txt).

   Le fichier d'activation est valide 60 minutes. Si vous attendez plus de 60 minutes avant d'utiliser le fichier d'activation, vous devez télécharger un nouveau fichier d'activation. Seul le dernier fichier d'activation est valide.

**À la fin :** Installer et configurer BlackBerry Connectivity Node.

# Installer et configurer BlackBerry Connectivity Node

**Avant de commencer :** Télécharger les fichiers d'installation et d'activation de BlackBerry Connectivity Node.

1. Ouvrez le fichier d'installation (.exe) de BlackBerry Connectivity Node que vous avez téléchargé à partir de la console de gestion.

   Si un message Windows s'affiche pour vous demander l'autorisation d'apporter des modifications sur l'ordinateur, cliquez sur **Oui**.
2. Choisissez votre langue. Cliquez sur **OK**.
3. Cliquez sur **Suivant**.
4. Sélectionnez votre pays ou région. Lisez et acceptez le contrat de licence. Cliquez sur **Suivant**.
5. Le programme d'installation vérifie que votre ordinateur répond aux exigences d'installation. Cliquez sur **Suivant**.
6. Pour modifier le chemin du fichier d'installation, cliquez sur **...** et accédez au chemin d'accès du fichier que vous souhaitez utiliser. Si vous recevez un message vous invitant à créer des dossiers pour les fichiers d'installation et les fichiers journaux, cliquez sur **Oui**. Cliquez sur **Suivant**.
7. Dans la boite de dialogue **Compte de service**, saisissez le mot de passe du compte de service. Cliquez sur **Installer**.
8. Lorsque l'installation est terminée, cliquez sur **Suivant**.

   L'adresse de la console BlackBerry Connectivity Node s'affiche (http:/localhost:8088). Cliquez sur le lien et enregistrez le site dans votre navigateur.
9. Sélectionnez votre langue. Cliquez sur **Suivant**.
10. Lorsque vous activez BlackBerry Connectivity Node, celui-ci envoie les données via le port 443 (HTTPS) à BlackBerry Infrastructure (par exemple na.bbsecure.com ou eu.bbsecure.com). Une fois activé, BlackBerry Connectivity Node utilise le port 3101 (TCP) pour toutes les autres connexions sortantes via BlackBerry Infrastructure. Effectuez l'une des opérations suivantes :

    - Si vous souhaitez utiliser un paramètre de proxy autre que celui par défaut (port 443) pour vous connecter à BlackBerry Infrastructure (<*région*>.bbsecure.com) afin d'activer BlackBerry Connectivity Node, cliquez sur le lien « ici » pour configurer les paramètres de proxy, puis saisir les informations concernant le proxy d'inscription. Ce lien n'est disponible que sur l'écran « Nommer votre BlackBerry Connectivity Node ». Si vous ne configurez pas les paramètres de proxy à partir de cet écran et cliquez sur **Suivant**, vous pouvez configurer les paramètres de proxy dans le coin supérieur droit de l'écran en cliquant sur **Paramètres > Proxy** avant de l'activer.

      **Remarque :** Le proxy doit être en mesure d'accéder au port 443 vers BlackBerry Infrastructure. Vous ne pouvez plus modifier le paramètre de proxy d'inscription après avoir activé BlackBerry Connectivity Node.
    - Configurez les autres paramètres proxy. Pour plus d'informations sur les options de proxy disponibles, reportez-vous à la rubrique Configurer les paramètres de proxy pour une BlackBerry Connectivity Node instance.
11. Dans le champ **Nom convivial**, saisissez un nom pour BlackBerry Connectivity Node. Cliquez sur **Suivant**.
12. Cliquez sur **Parcourir**. Sélectionnez le fichier d'activation que vous avez téléchargé à partir de la console de gestion.
13. Cliquez sur **Activer**.

    Si vous souhaitez ajouter une instance de BlackBerry Connectivity Node à un groupe de serveurs existant lorsque vous l'activez, le pare-feu de votre organisation doit autoriser les connexions à partir de ce serveur sur le port 443 via BlackBerry Infrastructure (par exemple na.bbsecure.com ou eu.bbsecure.com) pour activer BlackBerry Connectivity Node et dans la même région bbsecure.com que l'instance principale de BlackBerry Connectivity Node.
14. Cliquez sur + et sélectionnez le type de répertoire d'entreprise que vous souhaitez configurer.
15. Liez votre répertoire à BlackBerry Connectivity Node en suivant la tâche appropriée :

    - Connexion à Microsoft Active Directory
    - Se connecter à un annuaire LDAP

**À la fin :**

- Pour installer une deuxième instance de BlackBerry Connectivity Node pour la redondance, téléchargez un autre jeu de fichiers d'installation et d'activation et répétez cette tâche sur un autre ordinateur. Cette opération doit être effectuée après l'activation de la première instance.
- Vous pouvez configurer une ou plusieurs connexions de répertoire, mais si vous avez plusieurs BlackBerry Connectivity Node, toutes les connexions au répertoire doivent être configurées de la même manière. Si une connexion au répertoire est manquante ou mal configurée, ce BlackBerry Connectivity Node apparaît comme désactivé dans la console de gestion. Vous pouvez faciliter cette tâche en copiant les configurations de connexion de répertoire d'un BlackBerry Connectivity Node à un autre.
- Pour modifier les paramètres de répertoire que vous avez configurés, dans la console BlackBerry Connectivity Node (http:/localhost:8088), cliquez sur **Paramètres généraux > Répertoire d'entreprise**. Cliquez sur pour la connexion au répertorie.
- Configurez la journalisation de BlackBerry Connectivity Node.
- Vous pouvez supprimer des connexions au répertoire d'un BlackBerry Connectivity Node tant qu'aucun utilisateur ou groupe n'y est associé. Si vous supprimez une connexion d'un BlackBerry Connectivity Node, vous pouvez ajouter à nouveau la connexion en utilisant le même nom que la connexion supprimée.

# Copier les configurations de connexion au répertoire

Si votre environnement comporte plusieurs instances de BlackBerry Connectivity Node, les connexions au répertoire doivent être configurées de manière identique sur tous les nœuds. Pour faciliter cette tâche, vous pouvez exporter la configuration de la connexion au répertoire à partir d'un BlackBerry Connectivity Node et l'importer dans un autre.

**Remarque :** Avant de pouvoir importer des configurations de répertoire d'entreprise dans un BlackBerry Connectivity Node, vous devez supprimer toutes les connexions existantes au répertoire d'entreprise de ce nœud.

**Avant de commencer :** Copier les configurations de connexion au répertoire.

1. Dans le BlackBerry Connectivity Node à partir duquel vous souhaitez copier la configuration, sur l'écran **Connexion au répertoire d'entreprise**, cliquez sur **Exporter les connexions au répertoire dans un fichier .txt**.

   Un fichier .txt contenant des informations sur les connexions au répertoire d'entreprise est téléchargé sur votre ordinateur.
2. Sur le BlackBerry Connectivity Node vers lequel vous souhaitez copier la configuration, sur l'écran **Connexion au répertoire d'entreprise**, accédez au fichier .txt que vous avez téléchargé.
3. Cliquez sur **Importer des connexions**.

   Les connexions au répertoire d'entreprise sont ajoutées à BlackBerry Connectivity Node.

# Configurer des paramètres proxy pour une instance de BlackBerry Connectivity Node

Vous pouvez configurer les composants de BlackBerry Connectivity Node pour envoyer les données via un serveur proxy TCP (transparent ou SOCKS v5) avant d'atteindre BlackBerry Infrastructure.

1. Sur l'ordinateur qui héberge BlackBerry Connectivity Node, ouvrez la console BlackBerry Connectivity Node depuis le menu Démarrer ou ouvrez un navigateur et accédez à http://localhost:8088.
2. Cliquez sur **Paramètres généraux > Proxy**.
3. Effectuez l'une des tâches suivantes :

| Tâche | Étapes |
| --- | --- |
| Envoyez des données via un serveur proxy SOCKS v5 ( pas d'authentification) vers BlackBerry Infrastructure. | **a.** Sélectionnez l'option **Serveur proxy**.<br>**b.** Cochez la case **Activer SOCKS v5**.<br>**c.** Cliquez sur **+**.<br>**d.** Saisissez l'adresse IP ou le nom d'hôte du serveur proxy SOCKS v5. Cliquez sur **Ajouter**.<br>**e.** Répétez les étapes 3 et 4 pour chaque serveur proxy SOCKS v5 que vous souhaitez configurer.<br>**f.** Dans le champ **Port**, saisissez le numéro de port.<br>**g.** Cliquez sur **Enregistrer**. |
| Envoyez des données via un serveur proxy transparent vers BlackBerry Infrastructure. | • Dans les champs **BlackBerry Connectivity Node**, saisissez le nom de domaine complet ou l'adresse IP et le numéro de port du serveur proxy. |

4. Cliquez sur **Enregistrer**.

# Association à votre annuaire d'entreprise

Vous pouvez configurer Cylance Endpoint Security pour qu'il se synchronise avec le répertoire de votre entreprise afin de simplifier l'ajout et la gestion des utilisateurs et des groupes. Lorsque vous connectez Cylance Endpoint Security à un répertoire d'entreprise, vous pouvez créer des comptes d'utilisateur en recherchant et en important des données utilisateur depuis le répertoire d'entreprise. Les utilisateurs créés via la synchronisation de répertoire peuvent être activés pour l'application CylancePROTECT Mobile, CylanceGATEWAY et CylanceAVERT.

Vous pouvez créer un lien vers un répertoire d'entreprise de deux manières :

- Pour effectuer une synchronisation avec Microsoft Entra ID, vous pouvez configurer Cylance Endpoint Security pour qu'il s'y connecte.
- Pour effectuer une synchronisation avec un annuaire LDAP ou Microsoft Active Directory sur site, vous devez d'abord installer BlackBerry Connectivity Node pour créer une connexion sécurisée entre Cylance Endpoint Security et votre répertoire.

Pour connecter Cylance Endpoint Security à votre annuaire d'entreprise, procédez comme suit :

| Étape | Action |
|---|---|
| 1 | Si vous souhaitez créer un lien vers un répertoire d'entreprise sur site, installez un BlackBerry Connectivity Node. |
| 2 | Selon le type de répertoire auquel vous souhaitez vous connecter, configurez Cylance Endpoint Security pour la synchronisation avec Entra , ou connectez-vous à un Microsoft Active Directory ou à un annuaire LDAP. |
| 3 | Ajouter un groupe d'annuaires. |
| 4 | Configurer l'intégration et la suppression. |
| 5 | Configurer les plannings de synchronisation des annuaires. |

# Configurer Cylance Endpoint Security pour la synchronisation avec EntraActive Directory

Pour configurer Cylance Endpoint Security pour la synchronisation avec Entra Active Directory, vous devez configurer Entra et Cylance Endpoint Security pour établir la connexion.

1. Connectez-vous au portail Azure.
2. Créez un nouvel enregistrement d'application pour Entra Active Directory, et attribuez les paramètres et autorisations appropriés.
   a) Ajoutez un nom pour l'application.
   b) Sélectionnez les types de compte qui peuvent utiliser l'application ou accéder à l'API.
   c) Sélectionnez **Web** comme type d'URI de redirection et définissez l'URI sur `http://localhost`.
   d) Définissez les autorisations d'application suivantes :

- Group.Read.All (Application)
- User.Read (Délégué)
- User.Read.All (Application)

e) Accordez l'autorisation de l'administrateur à l'application.

3. Enregistrez le nom que vous avez attribué à l'application et l'ID de l'application (client).
4. Créez un nouveau secret de client et enregistrez l'information dans la colonne Valeur du secret.

   **Important :** La valeur n'est disponible que lorsque vous la créez. Vous ne pouvez pas y accéder après avoir quitté la page. Si vous n'enregistrez pas la valeur, vous devez en créer une nouvelle. Celle-ci est utilisée comme secret de client dans la console de gestion.
5. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Connexions au répertoire**.
6. Cliquez sur **Ajouter une nouvelle connexion**.
7. Saisissez un **Nom** pour la connexion au répertoire et le **Domaine** pour votre Entra Active Directory.
8. Dans le champ **ID client**, saisissez l'ID d'application généré par l'enregistrement de l'application Entra.
9. Dans le champ **Secret de client**, saisissez la valeur de secret de client générée à la suite de l'enregistrement de l'application Entra à l'étape 4.
10. Cliquez sur **Ajouter**.

## Mettre à jour les identifiants de connexion de Microsoft Entra ID Active Directory

Vous devez mettre à jour les informations d'identification du client dans la console de gestion lorsque votre secret de client a expiré ou a été modifié dans le portail Azure. En cas d'expiration ou de modification de votre secret de client, le symbole  s'affiche sur l'écran Connexions au répertoire en regard de la connexion au répertoire concernée. Vous pouvez choisir de mettre à jour uniquement le secret de client, ou à la fois l'ID de client et le secret de client.

**Avant de commencer :**

- Vérifiez que vous avez enregistré le nom que vous avez attribué à l'application dans Configurer Cylance Endpoint Security pour la synchronisation avec EntraActive Directory.
- Assurez-vous que vous disposez d'un secret de client valide et que vous avez enregistré les informations dans la colonne Valeur du secret. Vous pouvez éventuellement créer un nouvel ID de client et un nouveau secret de client.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Connexions au répertoire**.
2. Cliquez sur la connexion Microsoft Entra ID Active Directory à mettre à jour.
3. Cliquez sur l'onglet **Paramètres des connexions**.
4. Cliquez sur **Mettre à jour les informations d'identification du client**. Choisissez de mettre à jour uniquement le secret de client, ou l'ID de client et le secret de client. Effectuez l'une des opérations suivantes :
   - Mettre à jour le secret de client uniquement : saisissez la valeur du secret de client que vous avez enregistrée sur le portail Azure.
   - Mettre à jour l'ID de client et le secret de client : saisissez les nouvelles valeurs d'ID de client et de secret de client que vous avez enregistrées sur le portail Azure.
5. Cliquez sur **Envoyer**.
6. Cliquez sur **Enregistrer**. En cas d'échec de l'enregistrement, les valeurs précédentes d'ID de client et de secret de client sont rétablies.

# Connexion à Microsoft Active Directory

**Avant de commencer :** Installez au moins une instance de BlackBerry Connectivity Node.

1. Dans la BlackBerry Connectivity Node console (http:/localhost:8088), cliquez sur **Paramètres généraux > Répertoire d'entreprise**.
2. Cliquez sur +.
3. Sélectionnez **Microsoft Active Directory**.
4. Dans le champ **Nom de connexion**, saisissez un nom pour cette connexion au répertoire d'entreprise.
5. Dans le champ **Nom d'utilisateur**, saisissez le nom d'utilisateur du compte Microsoft Active Directory.
6. Dans le champ **Domaine**, saisissez le FQDN du domaine qui héberge Microsoft Active Directory. Par exemple : domain.example.com.
7. Dans le champ **Mot de passe**, saisissez le mot de passe du compte Microsoft Active Directory.
8. Dans la liste déroulante **Détection du contrôleur de domaine**, cliquez sur l'une des opérations suivantes :
   - Si vous souhaitez utiliser la détection automatique, cliquez sur **Automatique**.
   - Si vous souhaitez spécifier l'ordinateur du contrôleur de domaine, cliquez sur **Sélectionner dans la liste ci-dessous**. Cliquez sur + et saisissez le FQDN de l'ordinateur. Répétez cette étape pour ajouter d'autres ordinateurs.
9. Dans le champ **Base de recherche du catalogue global**, saisissez la base de recherche à laquelle vous souhaitez accéder (par exemple, OU=Users,DC=example,DC=com). Pour effectuer des recherches dans le catalogue global, laissez le champ vide.
10. Dans la liste déroulante **Détection du catalogue global**, cliquez sur l'une des opérations suivantes :
    - Si vous souhaitez utiliser la détection automatique de catalogue, cliquez sur **Automatique**.
    - Si vous souhaitez spécifier l'ordinateur du catalogue, cliquez sur **Sélectionner dans la liste ci-dessous**. Cliquez sur + et saisissez le FQDN de l'ordinateur. Répétez cette étape pour ajouter d'autres ordinateurs, si nécessaire
11. Si vous voulez activer la prise en charge de boites aux lettres Microsoft Exchange liées, dans la liste déroulante **Prise en charge des boites aux lettres Microsoft Exchange liées**, cliquez sur **Oui**. Pour configurer le compte Microsoft Active Directory de chacune des forêts auxquelles vous souhaitez accéder, dans la section **Liste des forêts de comptes**, cliquez sur +. Spécifiez le nom de la forêt, le nom du domaine de l'utilisateur (l'utilisateur peut appartenir à n'importe quel domaine de la forêt de comptes), le nom d'utilisateur et le mot de passe.
12. Pour synchroniser plus d'informations utilisateur à partir de votre annuaire d'entreprise, cochez la case **Synchroniser les informations complémentaires sur l'utilisateur**. Les informations supplémentaires comprennent le nom de l'entreprise et le téléphone du bureau.
13. Cliquez sur **Enregistrer**.

**À la fin :**

- Si vous souhaitez configurer l'intégration automatique pour Cylance Endpoint Security, reportez-vous à la section Configurer l'intégration et la suppression.
- Si vous souhaitez ajouter un calendrier de synchronisation du répertoire, reportez-vous à Configurer les plannings de synchronisation des annuaires.
- Si vous disposez de plusieurs instances de BlackBerry Connectivity Node, vous pouvez copier les configurations de connexion au répertoire d'une instance dans les autres.

# Se connecter à un annuaire LDAP

**Avant de commencer :** Pour vous connecter à un annuaire LDAP sur site, vous devez d'abord installer au moins une instance de BlackBerry Connectivity Node.

1. Dans la BlackBerry Connectivity Node console (http:/localhost:8088), cliquez sur **Paramètres généraux > Répertoire d'entreprise**.
2. Cliquez sur +.
3. Sélectionnez **LDAP**.
4. Dans le champ **Nom de connexion**, saisissez un nom pour cette connexion au répertoire d'entreprise.
5. Dans la liste déroulante **Détection du serveur LDAP**, cliquez sur l'une des opérations suivantes : si vous souhaitez utiliser la détection automatique, cliquez sur **Automatique**.
   - Si vous souhaitez utiliser la détection automatique, cliquez sur **Automatique**, puis dans le champ **Nom de domaine DNS**, saisissez le nom du domaine DNS.
   - Si vous souhaitez spécifier l'ordinateur LDAP, cliquez sur **Sélectionner le serveur dans la liste ci-dessous**. Cliquez sur + et saisissez le FQDN de l'ordinateur. Répétez cette étape pour ajouter d'autres ordinateurs.
6. Dans la liste déroulante **Activer SSL**, choisissez si vous souhaitez activer l'authentification SSL pour le trafic LDAP ou non. Si vous cliquez sur **Oui**, cliquez sur **Parcourir** et sélectionnez le certificat SSL pour l'ordinateur LDAP.
7. Dans le champ **Port LDAP**, saisissez le numéro de port de l'ordinateur LDAP.
8. Dans la liste déroulante **Autorisation requise**, sélectionnez si l'authentification est requise avec l'ordinateur LDAP. Si vous cliquez sur **Oui**, saisissez le nom d'utilisateur et le mot de passe du compte LDAP. Le nom d'utilisateur doit être en format DN (par exemple, CN=Megan Ball,OU=Sales,DC=example,DC=com).
9. Dans le champ **Base de recherche**, saisissez la base de recherche à laquelle vous souhaitez accéder (par exemple, OU=Users,DC=example,DC=com).
10. Dans le champ **Filtre de recherche de l'utilisateur LDAP**, saisissez le filtre que vous voulez utiliser pour les utilisateurs LDAP. Par exemple : (&(objectCategory=person)(objectclass=user)). Si vous souhaitez restreindre la recherche à tous les membres d'un seul groupe pour l'ensemble du locataire Cylance Endpoint Security, vous pouvez utiliser l'exemple suivant : (&(objectCategory=person)(objectclass=user)(memberOf=CN=Local,OU=Users,DC=example,DC=com)).
11. Dans la liste déroulante **Étendue de la recherche d'utilisateurs LDAP**, cliquez sur l'une des options suivantes : si vous souhaitez que les recherches d'utilisateurs s'appliquent à tous les niveaux en dessous du DN de base, cliquez sur **Tous les niveaux**. Si vous souhaitez limiter les recherches de l'utilisateur à un niveau en dessous du DN de base, cliquez sur **Un niveau**.
12. Dans le champ **Identificateur unique**, saisissez l'attribut de chaque identificateur unique de l'utilisateur (par exemple, uid). L'attribut doit être immuable et globalement unique pour chaque utilisateur.
13. Dans le champ **Prénom**, saisissez l'attribut du prénom de chaque utilisateur (par exemple, givenName).
14. Dans le champ **Nom**, saisissez l'attribut du nom de chaque utilisateur (par exemple, sn).
15. Dans le champ **Attribut de connexion**, saisissez l'attribut de connexion de chaque utilisateur (par exemple, cn).
16. Dans le champ **Adresse électronique**, saisissez l'attribut de messagerie de chaque utilisateur (par exemple, mail).
17. Dans le champ **Nom d'affichage**, saisissez l'attribut du nom d'affichage de chaque utilisateur (par exemple, displayName).
18. Pour synchroniser plus d'informations utilisateur à partir de votre annuaire d'entreprise, cochez la case **Synchroniser les informations complémentaires sur l'utilisateur**. Les informations supplémentaires comprennent le nom de l'entreprise et le téléphone du bureau.
19. Pour activer les groupes liés par répertoire, sélectionnez la case **Activer les groupes liés par répertoire**.

Spécifiez les informations suivantes :

- Dans le champ **Base de recherche de groupes**, saisissez la valeur à utiliser en tant que DN de base pour les recherches d'informations de groupe.
- Dans le champ **Filtre de recherche de groupes LDAP**, saisissez le filtre de recherche LDAP requis pour trouver des objets de groupe dans le répertoire de votre organisation.
- Dans le champ **Identifiant unique du groupe**, saisissez l'attribut de l'identifiant unique de chaque groupe. Cet attribut doit être immuable et globalement unique.
- Dans le champ **Nom d'affichage du groupe**, saisissez l'attribut du nom d'affichage de chaque groupe.
- Dans le champ **Attribut d'adhésion au groupe**, saisissez le nom de l'attribut d'adhésion au groupe. Les valeurs d'attribut doivent être au format DN.
- Dans le champ **Nom du groupe test**, saisissez un nom de groupe existant pour valider les attributs de groupe spécifiés.

**20.** Cliquez sur **Enregistrer**.

**À la fin :**

- Si vous souhaitez configurer l'intégration automatique pour Cylance Endpoint Security, reportez-vous à la section Configurer l'intégration et la suppression.
- Si vous souhaitez ajouter un calendrier de synchronisation du répertoire, reportez-vous à Configurer les plannings de synchronisation des annuaires.
- Si vous disposez de plusieurs instances de BlackBerry Connectivity Node, vous pouvez copier les configurations de connexion au répertoire d'une instance dans les autres.

# Configurer l'intégration et la suppression

L'intégration vous permet d'ajouter automatiquement des comptes d'utilisateur à Cylance Endpoint Security en fonction de l'appartenance des utilisateurs à un groupe de répertoires d'entreprise. Les groupes de répertoires et les comptes d'utilisateur sont ajoutés à CylanceGATEWAY lors du processus de synchronisation.

Si vous activez l'intégration, vous pouvez aussi choisir de configurer la suppression. Lorsqu'un utilisateur est désactivé dans le répertoire ou supprimé de tous les groupes de répertoires d'entreprise dans les groupes de répertoires d'intégration, Cylance Endpoint Security supprime le compte d'utilisateur et cesse d'autoriser les connexions réseau à partir des terminaux de l'utilisateur.

Vous pouvez utiliser la protection contre la suppression pour retarder la suppression des comptes d'utilisateur pour éviter toute suppression inattendue en raison de la latence de la réplication du répertoire. La protection contre la suppression retarde les actions de suppression de deux heures après le prochain cycle de synchronisation.

**Avant de commencer :** En fonction du type de répertoire auquel vous souhaitez vous connecter, configurez Cylance Endpoint Security pour qu'il se synchronise avec Azure Active Directory, ou connectez-vous à un répertoire Microsoft Active Directory ou à un répertoire LDAP.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Connexions à l'annuaire**.
2. Dans la liste **Connexions au répertoire**, cliquez sur la connexion pour laquelle vous souhaitez configurer l'intégration.
3. Dans l'onglet **Paramètres de synchronisation**, sélectionnez **Intégration de répertoire**.
4. Dans le champ **Synchronisation**, saisissez le nombre maximal de modifications à autoriser pour chaque synchronisation.

   Par défaut, il n'y a pas de limite. Si le nombre de modifications à synchroniser dépasse la limite définie, le processus de synchronisation s'arrête. Les modifications incluent les utilisateurs ajoutés aux groupes, les utilisateurs supprimés des groupes, les utilisateurs à intégrer et les utilisateurs à supprimer.

5. Dans le champ **Niveau d'imbrication**, saisissez le nombre de niveaux imbriqués à synchroniser pour les groupes de répertoires d'entreprise. Par défaut, il n'y a pas de limite.
6. Pour forcer la synchronisation des groupes de répertoires, sélectionnez **Forcer la synchronisation**.

   Si cette option est sélectionnée, lorsqu'un groupe est supprimé de votre répertoire d'entreprise, les liaisons vers ce groupe sont supprimées des groupes liés par répertoire et des groupes de répertoires d'intégration. Si cette case n'est pas cochée et qu'aucun répertoire d'entreprise n'est trouvé, le processus de synchronisation est annulé.
7. Pour supprimer un compte d'utilisateur de Cylance Endpoint Security lorsqu'un utilisateur est supprimé de tous les groupes liés dans le répertoire, sélectionnez **Supprimer l'utilisateur lorsqu'il est supprimé de tous les groupes de répertoires d'intégration**. La première fois qu'un cycle de synchronisation se produit après la suppression d'un compte d'utilisateur de tous les groupes de répertoires liés, le compte d'utilisateur est supprimé de Cylance Endpoint Security.
8. Pour empêcher la suppression inattendue de comptes d'utilisateur ou de données de terminaux de Cylance Endpoint Security, sélectionnez **Protection contre la suppression**.

   La protection contre la suppression signifie que les utilisateurs ne seront pas supprimés de Cylance Endpoint Security avant l'expiration d'un délai de deux heures après le cycle de synchronisation suivant.
9. Cliquez sur **Enregistrer**.

# Configurer les plannings de synchronisation des annuaires

Vous pouvez ajouter un planning pour synchroniser automatiquement Cylance Endpoint Security avec l'annuaire d'entreprise de votre organisation.

**Avant de commencer :** Connexion à Microsoft Active Directory ou Se connecter à un annuaire LDAP.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Connexions à l'annuaire**.
2. Dans la liste **Connexions à l'annuaire**, cliquez sur la connexion pour laquelle vous souhaitez définir un planning de synchronisation.
3. Dans l'onglet **Planning de synchronisation**, cliquez sur **Ajouter un planning**.
4. Dans la liste déroulante **Type de synchronisation**, sélectionnez l'une des options suivantes :

   - **Tous les groupes et utilisateurs** : il s'agit du paramètre par défaut. Si vous choisissez cette option et que l'intégration est activée, les utilisateurs sont intégrés, supprimés et liés aux groupes reliés à l'annuaire approprié pendant la synchronisation. Les utilisateurs qui ne sont pas intégrés ou supprimés, mais qui changent de groupe d'annuaire, et les utilisateurs dont les attributs sont modifiés, sont synchronisés.
   - **Groupes d'intégration** : si vous choisissez cette option et que l'intégration est activée, les utilisateurs sont intégrés, supprimés et liés aux groupes reliés à l'annuaire approprié au cours de la synchronisation, et les utilisateurs dont les attributs ont été modifiés sont synchronisés. Les utilisateurs qui ne sont pas intégrés ou supprimés, mais dont les groupes d'annuaire ont été modifiés ne sont pas synchronisés.
   - **Groupes reliés à l'annuaire** : si vous choisissez cette option les utilisateurs ne sont pas intégrés et supprimés lors de la synchronisation. Les utilisateurs dont les groupes reliés à l'annuaire ont été modifiés sont liés de manière appropriée. Les utilisateurs dont les attributs ont été modifiés sont synchronisés.
   - **Attributs de l'utilisateur** : si vous choisissez cette option les utilisateurs ne sont pas intégrés et supprimés lors de la synchronisation. Les utilisateurs dont les groupes d'annuaire ont été modifiés ne sont pas synchronisés. Les utilisateurs dont les attributs ont été modifiés sont synchronisés.
5. Dans la liste déroulante **Récurrence**, sélectionnez l'une des options suivantes :

   - **Intervalle** : il s'agit du paramètre par défaut. Si vous choisissez cette option, vous pouvez spécifier le nombre de minutes entre les synchronisations ainsi que les heures et les jours d'exécution de la synchronisation.

- **Une fois par jour** : si vous choisissez cette option, vous pouvez spécifier les jours de la semaine et l'heure d'exécution de la synchronisation.
- **Aucune récurrence** : si vous choisissez cette option, vous pouvez spécifier un jour et une heure au cours de la semaine suivante pour exécuter une synchronisation.

6. Spécifiez les informations de jour et d'heure appropriées pour le planning.
7. Cliquez sur **Envoyer**.
8. Cliquez sur **Enregistrer**.

# Synchroniser avec votre annuaire d'entreprise

Vous pouvez synchroniser Cylance Endpoint Security avec vos connexions au répertoire à tout moment.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Connexions à l'annuaire**.
2. Dans la liste **Connexions au répertoire**, cliquez sur pour la connexion à synchroniser.

# Configuration des administrateurs

Vous pouvez contrôler la façon dont les administrateurs accèdent à la console de gestion et l'utilisent en leur attribuant des rôles prédéfinis ou personnalisés. Ce contrôle d'accès basé sur les rôles vous permet d'accorder aux administrateurs l'accès aux fonctions spécifiques de la console dont ils ont besoin pour leur rôle et de limiter les fonctionnalités auxquelles vous ne souhaitez pas qu'ils aient accès.

Pour plus d'informations sur les rôles et les autorisations d'accès, consultez Autorisations pour les rôles d'administrateur.

## Ajouter un administrateur

Vous pouvez ajouter des utilisateurs administrateurs à la console de gestion pour leur permettre de contrôler et de configurer votre environnement Cylance Endpoint Security. Les comptes administrateur existants et nouvellement ajoutés s'affichent sur la page utilisateur (Actifs > Utilisateurs) de la console de gestion. Vous pouvez ajouter la colonne Administrateur pour afficher une icône en regard de chaque compte administrateur. Les écrans qu'un utilisateur administrateur peut afficher dans la console de gestion, et les fonctionnalités que l'utilisateur peut configurer et modifier, dépendent du rôle que vous attribuez à cet utilisateur. Pour plus d'informations sur les rôles et les autorisations d'accès, consultez Autorisations pour les rôles d'administrateur.

1. Sur la barre de menus de la console de gestion, cliquez sur **Paramètres > Administrateurs**. Effectuez l'une des opérations suivantes :

| Tâche | Étapes |
| --- | --- |
| Ajoutez un nouvel administrateur. | **a.** Sous **Ajouter des utilisateurs**, dans le champ **Saisir l'adresse électronique**, saisissez l'adresse électronique de l'utilisateur.<br>**b.** Dans la liste déroulante Sélectionner le rôle, cliquez sur un rôle. Pour en savoir plus sur les rôles et leurs autorisations associées, consultez la section Gestion des rôles.<br>**c.** Si vous avez sélectionné un gestionnaire de zone ou un rôle d'utilisateur, cliquez sur une zone dans la liste déroulante **Sélectionner la zone**.<br>**d.** Cliquez sur **Ajouter**.<br>Cylance Endpoint Security envoie un e-mail au nouvel utilisateur administrateur avec un lien pour créer un mot de passe. |

| Tâche | Étapes |
| --- | --- |
| Modifiez un rôle d'administrateur. | **a.** Cliquez sur un utilisateur administrateur.<br>**b.** Dans la liste déroulante, cliquez sur un nouveau rôle.<br>**c.** Si vous avez sélectionné le rôle Responsable de zone ou Utilisateur, procédez comme suit :<br>**1.** Choisissez le **Rôle de zone par défaut** à attribuer à l'utilisateur lors de la création d'une nouvelle zone. La valeur par défaut est « Aucun ».<br>**2.** Réglez le rôle de l'utilisateur pour chaque zone en conséquence.<br>Notez que si un utilisateur se voit attribuer le rôle de Gestionnaire de zone pour au moins une zone, il héritera de certaines fonctionnalités du gestionnaire de zone, telles que la possibilité d'afficher la liste des stratégies de terminal, de télécharger le programme d'installation et d'afficher la liste globale. Cependant, l'utilisateur ne peut exécuter les fonctions de gestionnaire de zone que sur les terminaux situés dans les zones dans lesquelles le rôle de gestionnaire de zone lui est attribué. De même, l'utilisateur ne peut exécuter les fonctions Utilisateur que sur les terminaux situés dans les zones où le rôle utilisateur lui est attribué.<br>**d.** Dans la fenêtre contextuelle, saisissez votre mot de passe.<br>**e.** Cliquez sur **Enregistrer**. |

2. Dans la barre de menus, cliquez sur **Actifs > Utilisateurs**. Effectuez l'une des opérations suivantes :
   - Pour ajouter ou supprimer des colonnes, cliquez sur ||| et sélectionnez les colonnes que vous souhaitez afficher.
   - Pour trier les utilisateurs dans l'ordre croissant ou décroissant par colonne, cliquez sur la colonne.
   - Pour filtrer les utilisateurs par colonne, utilisez le champ de filtre et l'icône de la colonne.
   - Pour afficher uniquement les comptes administrateur, cliquez sur ⏷ et définissez l'option Administrateur sur **Vrai**.

# Autorisations pour les rôles d'administrateur

Les tableaux suivants répertorient les autorisations par défaut pour les rôles définis par le système au sein de la console de gestion. Les autorisations en gras possèdent des autorisations enfants disponibles uniquement après la sélection de l'autorisation principale.

Les données que les gestionnaires de zone peuvent afficher dans la console sont limitées aux zones qu'ils gèrent.

#### Tableau de bord

Ces autorisations fournissent un accès à la page du tableau de bord et ne peuvent pas être désactivées. Des informations affichées sur le tableau de bord sont déterminées par le rôle et les autorisations attribués au rôle d'administrateur.

| Autorisation | Administrateur | Gestionnaire de zone | Utilisateur | Lecture seule |
|---|---|---|---|---|
| **Protection de terminal** | √ | √ | √ | √ |

#### Réponse de détection de point de terminaison

Ces autorisations vous permettent de gérer les fonctionnalités CylanceOPTICS.

| Autorisation | Administrateur | Gestionnaire de zone | Utilisateur | Lecture seule |
|---|---|---|---|---|
| **Afficher les détections** | √ | √ | | √ |
| Modifier des détections | √ | √ | | |
| Supprimer des détections | √ | √ | | |
| **Afficher, créer InstaQuery** | √ | √ | | √ |
| Supprimer la requête InstaQuery | √ | √ | | |
| **Afficher, créer une requête avancée** | √ | √ | | √ |
| Créer un modèle partagé | √ | √ | | |
| Supprimer un modèle partagé | √ | | | |
| Supprimer des instantanés partagés | √ | | | |
| Supprimer une requête d'exportation partagée | √ | | | |
| Créer une requête planifiée | √ | √ | | |
| Modifier une requête planifiée partagée | √ | | | |
| Supprimer une requête planifiée partagée | √ | | | |
| **Afficher, créer des données détaillées** | √ | √ | | √ |
| **Afficher le déploiement du package** | √ | | | √ |

| Autorisation | Administrateur | Gestionnaire de zone | Utilisateur | Lecture seule |
|---|---|---|---|---|
| Créer un déploiement de package | √ | | | |
| Mettre à jour un déploiement de package | √ | | | |
| Supprimer un déploiement de package | √ | | | |
| **Afficher les résultats du playbook** | √ | | | √ |
| Supprimer les résultats du playbook | √ | | | |
| **Afficher le package** | √ | | | √ |
| Créer un package | √ | | | |
| Supprimer un package | √ | | | |
| **Afficher le playbook** | √ | | | √ |
| Créer, modifier un playbook | √ | | | |
| Supprimer un playbook | √ | | | |
| **Afficher le jeu de règles*** | √ | | | √ |
| Modifier un jeu de règles* | √ | | | |
| Supprimer un jeu de règles | √ | | | |
| **Afficher les règles** | √ | | | √ |
| Créer, modifier une règle personnalisée | √ | | | |
| Supprimer une règle personnalisée | √ | | | |
| **Afficher les exceptions** | √ | | | √ |
| Créer, modifier des exceptions | √ | | | |
| Supprimer des exceptions | √ | | | |

| Autorisation | Administrateur | Gestionnaire de zone | Utilisateur | Lecture seule |
|---|---|---|---|---|
| **Afficher la configuration du verrouillage** | √ | | | √ |
| Créer, modifier une configuration de verrouillage | √ | | | |
| Supprimer une configuration de verrouillage | √ | | | |

*Pour afficher un jeu de règles, vous devez disposer d'un rôle d'administrateur avec les autorisations Afficher le jeu de règles et Modifier un jeu de règles.

#### Utilisateurs et terminaux

Ces autorisations contrôlent ce que vous pouvez faire avec les utilisateurs et les terminaux dans la console de gestion. Vous devez disposer d'autorisations de liste globale pour effectuer une mise en quarantaine globale ou ajouter une menace à la liste sécurisée depuis ces pages.

| Autorisation | Administrateur | Gestionnaire de zone | Utilisateur | Lecture seule |
|---|---|---|---|---|
| **Afficher les utilisateurs et les groupes** | √ | | | √ |
| Créer des utilisateurs et des groupes | √ | | | |
| Modifier les utilisateurs et les groupes | √ | | | |
| Supprimer des utilisateurs et des groupes | √ | | | |
| **Afficher les terminaux mobiles** | √ | | | √ |
| Supprimer les terminaux mobiles | √ | | | |
| **Afficher les terminaux** | √ | √ | √ | √ |
| Modifier les terminaux | √ | √ | | |
| Supprimer des terminaux | √ | | | |

| Autorisation | Administrateur | Gestionnaire de zone | Utilisateur | Lecture seule |
|---|---|---|---|---|
| Exécuter l'analyse d'arrière-plan | √ | | | |
| Verrouiller un terminal CylanceOPTICS | √ | | | |
| Déverrouiller un terminal CylanceOPTICS | √ | | | |
| Exécuter une réponse distante | √ | | | |
| Autoriser le téléchargement d'un fichier | √ | | | |
| **Afficher les stratégies de terminal** | √ | √ | | √ |
| Créer des stratégies de terminal | √ | | | |
| Modifier les stratégies de terminal | √ | | | |
| Supprimer des stratégies de terminal | √ | | | |
| **Afficher les zones** | √ | √ | √ | √ |
| Créer des zones | √ | | | |
| Modifier les zones | √ | √ | | |
| Supprimer des zones | √ | | | |

#### Protection contre les menaces

Ces autorisations permettent d'accéder au menu Protection, aux alertes CylancePROTECT Mobile et aux vulnérabilités.

| Autorisation | Administrateur | Gestionnaire de zone | Utilisateur | Lecture seule |
|---|---|---|---|---|
| **Afficher la protection contre les menaces** | √ | √ | √ | √ |
| Modifier des évènements Protect Mobile | √ | | | |

| Autorisation | Administrateur | Gestionnaire de zone | Utilisateur | Lecture seule |
|---|---|---|---|---|
| **Afficher les stratégies Protect Mobile** | √ | | | √ |
| Créer des stratégies Protect Mobile | √ | | | |
| Modifier des stratégies Protect Mobile | √ | | | |
| Supprimer des stratégies Protect Mobile | √ | | | |

#### Réseau

Ces autorisations vous permettent de gérer les paramètres de protection réseau, y compris le contrôle d'accès au réseau, les paramètres CylanceGATEWAY ainsi que les alertes et les événements CylanceGATEWAY.

| Autorisation | Administrateur | Gestionnaire de zone | Utilisateur | Lecture seule |
|---|---|---|---|---|
| **Afficher les stratégies du service Gateway** | √ | | | √ |
| Créer des stratégies du service Gateway | √ | | | |
| Modifier des stratégies du service Gateway | √ | | | |
| Supprimer des stratégies du service Gateway | √ | | | |
| **Afficher les contrôles d'accès réseau** | √ | | | √ |
| Modifier les contrôles d'accès réseau | √ | | | |
| **Afficher les paramètres Gateway** | √ | | | √ |
| Créer des paramètres Gateway | √ | | | |
| Modifier des paramètres Gateway | √ | | | |

| Autorisation | Administrateur | Gestionnaire de zone | Utilisateur | Lecture seule |
|---|---|---|---|---|
| Supprimer des paramètres Gateway | √ | | | |
| **Afficher les événements de rapport Gateway** | √ | | | √ |
| **Afficher les alertes et événements Gateway** | √ | | | √ |

#### Avert

Ces autorisations vous permettent de gérer les fonctionnalités CylanceAVERT.

| Autorisation | Administrateur | Gestionnaire de zone | Utilisateur | Lecture seule |
|---|---|---|---|---|
| **Afficher les paramètres Avert** | √ | | | √ |
| Modifier les paramètres Avert | √ | | | |
| **Afficher l'identifiant de terminal Avert** | √ | | | √ |
| **Afficher les scores de risque Avert** | √ | | | √ |
| **Afficher les évènements de terminal Avert** | √ | | | √ |
| **Afficher les stratégies Avert** | √ | | | √ |
| Créer des stratégies Avert | √ | | | |
| Modifier les stratégies Avert | √ | | | |
| Supprimer des stratégies Avert | √ | | | |
| **Afficher le résumé des fichiers sensibles Avert** | √ | | | |
| Afficher le contenu du fichier Avert | √ | | | |
| Supprimer les fichiers Avert | √ | | | |

#### Commun

Ces autorisations permettent aux administrateurs de gérer les paramètres au niveau du locataire qui affectent plusieurs fonctionnalités dans la solution Cylance Endpoint Security, notamment les répertoires et les fournisseurs EMM, l'inscription des terminaux mobiles ainsi que les événements et les options de risques adaptatifs CylanceGATEWAY. Pour les connexions aux répertoires, vous pouvez uniquement créer des Active Directories (AD) Microsoft Entra ID.

| Autorisation | Administrateur | Gestionnaire de zone | Utilisateur | Lecture seule |
|---|---|---|---|---|
| **Afficher les connexions EMM** | √ | | | √ |
| Créer des connexions EMM | √ | | | |
| Modifier les connexions EMM | √ | | | |
| Supprimer des connexions EMM | √ | | | |
| **Afficher les connexions au répertoire** | √ | | | √ |
| Créer des connexions au répertoire | √ | | | |
| Modifier les connexions au répertoire | √ | | | |
| Supprimer des connexions au répertoire | √ | | | |
| **Afficher le connecteur de répertoire local** | √ | | | √ |
| Créer un connecteur de répertoire local | √ | | | |
| Modifier le connecteur de répertoire local | √ | | | |
| Supprimer le connecteur de répertoire local | √ | | | |
| **Afficher les contrôles d'authentification** | √ | | | √ |
| Créer des authentificateurs | √ | | | |
| Modifier des authentificateurs | √ | | | |

| Autorisation | Administrateur | Gestionnaire de zone | Utilisateur | Lecture seule |
|---|---|---|---|---|
| Supprimer des authentificateurs | √ | | | |
| **Afficher les stratégies d'inscription** | √ | | | √ |
| Créer des stratégies d'inscription | √ | | | |
| Modifier les stratégies d'inscription | √ | | | |
| Supprimer des stratégies d'inscription | √ | | | |
| **Afficher les stratégies de risque adaptatif** | √ | | | √ |
| Créer des stratégies de risque adaptatif | √ | | | |
| Modifier les stratégies de risque adaptatif | √ | | | |
| Supprimer des stratégies de risque adaptatif | √ | | | |
| **Afficher les paramètres de risque adaptatif** | √ | | | √ |
| Créer des paramètres de risque adaptatif | √ | | | |
| Modifier les paramètres de risque adaptatif | √ | | | |
| Supprimer des paramètres de risque adaptatif | √ | | | |
| **Afficher les alertes** | √ | | | √ |
| Modifier les alertes | √ | | | |
| Supprimer les alertes | √ | | | |

#### Journalisation

Ces autorisations vous permettent d'afficher les rapports et le journal d'audit.

| Autorisation | Administrateur | Gestionnaire de zone | Utilisateur | Lecture seule |
|---|---|---|---|---|
| **Afficher les rapports** | √ | | | √ |
| **Afficher le fichier journal d'audit** | √ | | | √ |

#### Paramètres

Ces autorisations vous permettent de gérer les paramètres de la console de gestion. Les autorisations de gestion des utilisateurs et celles de gestion des rôles sont associées. Si un rôle est attribué à un utilisateur avec des autorisations de gestion des utilisateurs sélectionnées, l'utilisateur aura également accès à la fonctionnalité de gestion des rôles.

| Autorisation | Administrateur | Gestionnaire de zone | Utilisateur | Lecture seule |
|---|---|---|---|---|
| **Application** | √ | √ | | √ |
| Gestion de jeton | √ | | | |
| Téléchargement du programme d'installation | √ | √ | | |
| Désinstaller la gestion des mots de passe | √ | | | |
| Connexion à l'assistance | √ | | | |
| Syslog/SIEM | √ | | | |
| Authentification personnalisée | √ | | | |
| Rapport de données sur les menaces | √ | | | |
| **Gestion des utilisateurs** | √ | | | |
| **Afficher la liste globale** | √ | √ | | √ |
| Créer une liste globale | √ | | | |
| Modifier la liste globale | √ | | | |
| Supprimer la liste globale | √ | | | |
| **Afficher les paramètres de mise à jour de l'agent** | √ | | | √ |

| Autorisation | Administrateur | Gestionnaire de zone | Utilisateur | Lecture seule |
|---|---|---|---|---|
| Créer les paramètres de mise à jour de l'agent | √ | | | |
| Modifier les paramètres de mise à jour de l'agent | √ | | | |
| Supprimer les paramètres de l'agent | √ | | | |
| **Certificats** | √ | √ | | √ |
| **Intégrations** | √ | | | |
| **Afficher les paramètres de cycle de vie du terminal** | √ | | | √ |
| Créer des paramètres de cycle de vie de terminal | √ | | | |
| Modifier les paramètres de cycle de vie du terminal | √ | | | |
| Supprimer des paramètres de cycle de vie du terminal | √ | | | |
| **Afficher les paramètres d'activation** | √ | | | √ |
| Modifier les paramètres d'activation | √ | | | |

# Gestion des rôles

Vous pouvez utiliser des rôles prédéfinis ou créer des rôles personnalisés pour gérer l'accès administrateur aux fonctionnalités de la console de gestion. Les rôles prédéfinis ont établi des autorisations qui ne sont pas modifiables. En fonction des autorisations de votre rôle, certaines options de menu, pages et fonctionnalités peuvent ne pas être disponibles. Par exemple, si un utilisateur n'a pas accès à une fonctionnalité de zone, l'option de menu Zones ne s'affiche pas. L'écran Tableau de bord est disponible pour tous les rôles prédéfinis et personnalisés, mais les données qu'il affiche reflètent uniquement les zones que l'utilisateur connecté est autorisé à gérer.

Pour obtenir la liste complète des autorisations d'utilisateurs pour chaque rôle prédéfini, reportez-vous à Autorisations pour les rôles d'administrateur. Les utilisateurs affectés à un rôle personnalisé ne peuvent pas activer les notifications sur la page Mon compte.

## Ajouter un rôle

Les rôles personnalisés ont une portée globale et fournissent un accès opérationnel complet aux pages et actions associées à une zone définie. Par exemple, si un rôle personnalisé dispose d'autorisations pour les

fonctionnalités de zone, tout utilisateur affecté au rôle a accès à toutes les fonctionnalités disponibles sur les pages Zones ou Détails de la zone.

Si l'accès n'est pas sélectionné pour un rôle, les utilisateurs ne verront pas cette page dans le menu et ne pourront pas accéder à la page à partir d'autres emplacements de la console. Par exemple, si un rôle personnalisé dispose d'autorisations pour les menaces mais pas pour les terminaux, la page Protection contre les menaces s'affiche dans le menu tandis que la page Terminaux ne s'affiche pas. Si l'utilisateur affiche la page Détails de la menace pour une menace, les terminaux et zones concernés s'affichent, mais il reçoit une page d'erreur lorsqu'il tente de cliquer sur le lien pour obtenir des détails sur un terminal spécifique.

1. Sur la barre de menus de la console de gestion, cliquez sur **Paramètres > Administrateurs**.
2. Cliquez sur **Rôles**.
3. Cliquez sur **Ajouter un nouveau rôle**.
4. Saisissez un nom pour le rôle.
5. Cochez la case **Accès** près d'une fonction à laquelle ce rôle doit être autorisé à accéder. Développez les sections pour afficher plus d'options. Pour plus d'informations, reportez-vous à Autorisations pour les rôles d‘administrateur.
6. Cliquez sur **Ajouter un rôle**.

**À la fin :**

- Pour modifier un rôle existant, cliquez dessus et modifiez le nom ou les autorisations. Le nom ou les autorisations mis à jour seront appliqués à tous les utilisateurs affectés au rôle existant.
- Si des utilisateurs sont attribués à un rôle prédéfini ou personnalisé, vous pouvez cliquer sur la colonne **Utilisateurs attribués** pour afficher l'e-mail des utilisateurs affectés à ce rôle. Vous pouvez cliquer sur l'e-mail pour afficher la page Détails de cet utilisateur.
- Pour supprimer un rôle, cochez la case près d'un rôle auquel aucun utilisateur n'est affecté, puis cliquez sur **Supprimer**. Si des utilisateurs sont affectés à un rôle, vous ne pouvez pas cocher la case.

# Configurer la limite d‘expiration de session et d‘expiration en cas d‘inactivité

Vous pouvez spécifier la durée pendant laquelle un administrateur peut rester connecté à la console de gestion avant d‘être déconnecté, même si la session est active. Vous pouvez également spécifier la durée pendant laquelle une session est autorisée à rester inactive avant de déconnecter l‘administrateur de la console.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Authentification**.
2. Dans l‘onglet **Paramètres** de la section **Expiration de la console**, configurez la limite d'**expiration de session**.

   Quelques minutes avant d‘atteindre la limite d‘expiration de la console, un compte à rebours s‘affiche dans une invite sur l‘écran des administrateurs, ce qui leur permet de s‘authentifier à nouveau pour poursuivre la session. Si l‘administrateur ne répond pas activement à l‘invite en cliquant sur **Vérifier** et en se reconnectant, il est déconnecté à l‘expiration du délai.
3. Configurez la limite d'**expiration en cas d‘inactivité**.
4. Cliquez sur **Enregistrer**.

# Ajout d'utilisateurs et de terminaux

Vous devez ajouter des comptes d'utilisateur dans la console de gestion afin de pouvoir activer les services Cylance Endpoint Security suivants pour ces utilisateurs :

- Services disponibles dans l'application CylancePROTECT Mobile : CylancePROTECT Mobile et CylanceGATEWAY Mobile
- Desktop CylanceGATEWAY

Vous pouvez utiliser les méthodes suivantes pour ajouter des utilisateurs :

- Établissez un lien vers le répertoire de votre entreprise et activez l'intégration pour ajouter automatiquement des utilisateurs lors de la synchronisation de Cylance Endpoint Security avec l'annuaire. Vous pouvez configurer les planifications de synchronisation de répertoire pour synchroniser Cylance Endpoint Security avec le répertoire de votre entreprise. Par défaut, tous les utilisateurs et groupes sont synchronisés tous les jours à des intervalles de 30 minutes.
- Établissez un lien vers le répertoire de votre entreprise et ajoutez des utilisateurs du répertoire de façon individuelle. Utilisez cette option si vous ne souhaitez pas activer l'intégration.
- Ajoutez des utilisateurs individuels en tant qu'utilisateurs BlackBerry Online Account.

Vous n'avez pas besoin d'ajouter de comptes d'utilisateur pour activer d'autres services Cylance Endpoint Security tels que CylancePROTECT Desktop et CylanceOPTICS. Une fois les agents installés sur les terminaux, vous pouvez afficher et gérer ces terminaux et les données associées dans la console de gestion.

## Ajouter l'application CylancePROTECT Mobile et des utilisateurs CylanceGATEWAY

**Avant de commencer :** Si vous souhaitez ajouter des utilisateurs à partir de votre répertoire d'entreprise, suivez les instructions fournies dans la section Association à votre annuaire d'entreprise. Si vous activez l'intégration, les groupes de répertoire et les comptes d'utilisateur sont ajoutés à la console de gestion pendant le processus de synchronisation. Suivez les étapes ci-dessous si vous souhaitez ajouter des utilisateurs de répertoire individuellement sans intégration, ou si vous souhaitez ajouter des utilisateurs individuels en tant qu'utilisateurs BlackBerry Online Account.

1. Dans la console de gestion, cliquez sur **Actifs > Utilisateurs** sur la barre de menu.
2. Cliquez sur **Ajouter des utilisateurs**.
3. Effectuez l'une des opérations suivantes :

| Tâche | Étapes |
| --- | --- |
| Ajoutez un utilisateur de répertoire. | **a.** Saisissez le nom de l'utilisateur et cliquez sur le résultat correspondant dans la liste déroulante.<br>**b.** Si vous avez déjà ajouté des groupes d'utilisateurs, vous pouvez également ajouter l'utilisateur à un ou plusieurs groupes. |

| Tâche | Étapes |
| --- | --- |
| Ajoutez un utilisateur BlackBerry Online Account. | **a.** Cliquez dans le champ de recherche et cliquez sur **Ajouter un nouvel utilisateur manuellement**. Si vous n'avez pas configuré de connexion au répertoire, passez à l'étape suivante.<br>**b.** Spécifiez le nom et l'adresse électronique de l'utilisateur.<br>**c.** Si vous avez déjà ajouté des groupes d'utilisateurs, vous pouvez également ajouter l'utilisateur à un ou plusieurs groupes.<br>**d.** Dirigez l'utilisateur vers la réinitialisation du mot de passe BlackBerry Online Account pour saisir son adresse électronique et définir un mot de passe. L'utilisateur utilisera ce mot de passe pour activer l'application CylancePROTECT Mobile. Les utilisateurs peuvent également accéder au lien de réinitialisation du mot de passe à partir de l'application CylancePROTECT Mobile lorsqu'ils activent l'application. |

4. Cliquez sur **Enregistrer**. Si vous souhaitez ajouter un autre utilisateur, cliquez sur **Enregistrer et ajouter nouveau** et répétez l'étape précédente.

**À la fin :**

- Pour ajouter des utilisateurs à un groupe, dans **Actifs > Groupes d'utilisateurs**, sélectionnez le groupe et ajoutez des utilisateurs à celui-ci à partir de l'onglet **Utilisateurs**. Si vous avez activé l'intégration, l'adhésion au groupe est synchronisée à partir du répertoire.
- Pour activer CylancePROTECT Mobile pour les utilisateurs que vous avez ajoutés, suivez les instructions fournies dans la section Configurer CylancePROTECT Mobile.
- Pour activer CylanceGATEWAY pour les utilisateurs que vous avez ajoutés, suivez les instructions fournies dans la section Configurer CylanceGATEWAY.
- Attribuer des stratégies à des administrateurs, des utilisateurs et des groupes.

# Ajout de groupes d'utilisateurs

Vous pouvez créer des groupes pour les utilisateurs qui sont activés pour l'application CylancePROTECT Mobile et pour les utilisateurs CylanceGATEWAY. Un groupe d'utilisateurs est un ensemble d'utilisateurs partageant des propriétés communes. L'administration d'utilisateurs sous forme de groupe est plus efficace que l'administration d'utilisateurs individuels car elle permet d'ajouter des propriétés, de les modifier ou de les supprimer simultanément de tous les membres du groupe. Lorsque vous attribuez des stratégies à des groupes d'utilisateurs, elles s'appliquent à tous les membres du groupe.

Vous pouvez attribuer des stratégies à un groupe à partir de la page des paramètres de groupe ou de la page des stratégies. Si un utilisateur appartient à deux groupes ou plus auxquels des stratégies différentes sont attribuées, la stratégie attribuée ayant le classement le plus élevé est appliquée à l'utilisateur.

Vous pouvez créer deux types de groupes d'utilisateurs :

- Les groupes de répertoires lient les groupes à votre annuaire d'entreprise. L'appartenance au groupe est synchronisée avec la liste d'appartenance du répertoire. Pour plus d'informations, reportez-vous à Configurer l'intégration et la suppression.
- Les groupes locaux sont créés et gérés dans la console de gestion. Vous pouvez attribuer n'importe quel utilisateur local ou utilisateur de répertoire à un groupe local.

### Ajouter un groupe d'annuaires

Si vous avez lié un ou plusieurs annuaires d'entreprise et configuré l'intégration, les groupes d'annuaires peuvent être automatiquement ajoutés à Cylance Endpoint Security. Vous pouvez également ajouter un groupe d'annuaires s'il n'a pas été ajouté par le biais de l'intégration.

1. Dans la console de gestion, cliquez sur **Actifs > Groupes d'utilisateurs** sur la barre de menu.
2. Cliquez sur **Ajouter un groupe > Groupe d'annuaires**.
3. Commencez à saisir le nom d'un groupe tel qu'il apparait dans l'annuaire.
4. Sélectionnez le nom du groupe lorsqu'il apparait dans les résultats de la recherche.
5. Si vous souhaitez que le groupe et les groupes imbriqués soient activés pour l'intégration, sélectionnez **Groupes d'annuaires imbriqués**.
6. Pour attribuer une stratégie au groupe, cliquez sur ⊕ et sélectionnez le type de stratégie que vous souhaitez ajouter.
7. Sélectionnez la stratégie et cliquez sur **Enregistrer**.

### Ajouter un groupe local

1. Dans la console de gestion, cliquez sur **Actifs > Groupes d'utilisateurs** sur la barre de menu.
2. Cliquez sur **Ajouter un groupe > Groupe local**.
3. Saisissez un nom et une description pour le groupe.
4. Pour attribuer une stratégie au groupe, cliquez sur ⊕ et sélectionnez le type de stratégie que vous souhaitez ajouter.
5. Sélectionnez la stratégie et cliquez sur **Enregistrer**.
6. Lorsque vous avez terminé d'attribuer des stratégies, cliquez sur **Enregistrer**.
7. Pour ajouter des utilisateurs au groupe, sur la page **Groupes d'utilisateurs**, cliquez sur le nom du groupe, puis sur **Utilisateurs**.
8. Cliquez sur **Ajouter un utilisateur**.
9. Commencez à saisir un nom pour rechercher l'utilisateur que vous souhaitez ajouter.
10. Sélectionnez un ou plusieurs noms dans les résultats de la recherche.
11. Cliquez sur **Enregistrer**.

    Vous pouvez également ajouter et supprimer des utilisateurs individuels des groupes sur la page utilisateur.

# Ajouter un authentificateur

Vous ajoutez des authentificateurs afin de pouvoir les ajouter aux stratégies d'authentification. L'authentificateur définit généralement une méthode d'authentification, telle qu'un mot de passe (par exemple, un mot de passe de console Cylance) ou une connexion à un tiers pour une authentification telle que Active Directory, Okta, ou Ping Identity. Vous les ajoutez aux stratégies d'authentification pour spécifier les types d'authentification que les administrateurs doivent effectuer pour se connecter à la console Cylance et que les utilisateurs doivent effectuer pour activer des applications ou des agents Cylance Endpoint Security ( par exemple, l'application CylancePROTECT Mobile ou CylanceGATEWAY). Vous pouvez combiner plusieurs authentificateurs dans une stratégie d'authentification pour fournir plusieurs étapes d'authentification. Par exemple, vous pouvez combiner l'authentificateur Enterprise avec une invite de mot de passe à usage unique dans une stratégie pour obliger les utilisateurs à s'authentifier à la fois avec leur mot de passe de console Cylance ou de poste et un mot de passe à usage unique.

**Avant de commencer :**

- **Important :** Vérifiez que vous avez examiné et effectué les étapes appropriées pour l'Authentification améliorée pour la connexion sur la console Cylance avant de configurer votre authentificateur SAML IDP. Si les étapes requises ne sont pas effectuées, l'authentificateur tiers ne pourra pas communiquer avec Cylance Endpoint Security. Pour en savoir plus, consultez les sections suivantes :
  - Pour savoir comment configurer un IDP pour une authentification améliorée et un accès initié par IDP à la console Cylance, reportez-vous à la section Authentification améliorée pour la connexion.
  - Pour obtenir des instructions détaillées sur la configuration d'un nouveau SAML IDP, reportez-vous à la section Comment configurer des fichiers SAML IDP pour une authentification améliorée et un accès initié par IDP à la console Cylance.
  - Pour obtenir des instructions détaillées sur les étapes permettant d'activer l'accès initié par IDP à la console pour un SAML IDP existant créé avant décembre 2023, reportez-vous à la section Comment mettre à jour les authentificateurs IDP externes (SAML) pour SSO afin d'accéder à la console Cylance.
- Si vous ajoutez un authentificateur SAML, téléchargez un exemplaire du certificat de signature de votre IDP.

1. Sur la barre de menus, cliquez sur **Paramètres > Authentification**.
2. Cliquez sur **Ajouter un authentificateur**.
3. Dans la liste déroulante **Type d'authentificateur**, sélectionnez l'un des authentificateurs suivants :

| Élément | Description |
| --- | --- |
| Entra (SAML) | Sélectionnez cette option si vous souhaitez que les utilisateurs saisissent leurs informations d'identification Entra sur la page d'ouverture de session principale et activent l'accès initié par IDP à la console Cylance.<br><br>Pour connaître les étapes de configuration de votre Entra (SAML), reportez-vous aux sections suivantes :<br><br>• Configurer un nouveau Entra (SAML) : Configurer l'authentificateur Entra (SAML) pour une authentification améliorée<br>• Activer l'accès initié par Entra pour un Entra (SAML) existant : Mettre à jour l'authentificateur Entra (SAML) pour activer l'accès initié par IDP à la console Cylance<br><br>**Remarque :** L'URL de rappel SSO au format https://login.eid.blackberry.com/_/resume/saml20/*hash*> est générée lorsque vous enregistrez l'authentificateur.<br><br>Procédez comme suit :<br><br>**a.** Saisissez un nom pour l'authentificateur.<br>**b.** Si vous souhaitez que les utilisateurs valident leur adresse e-mail avec un code à usage unique lors de leur première connexion, activez **Validation requise**. Le code est envoyé à l'adresse e-mail associée à l'utilisateur dans votre locataire.<br>**c.** Dans le champ **URL de demande de connexion**, saisissez l'URL de connexion spécifiée dans les paramètres d'authentification unique d'enregistrement de l'application correspondant à votre fournisseur d'identité. Par exemple, sur le portail Entra, accédez à Application d'entreprise > *Name of the newly created application*> > section Configuration de *application name* > URL de connexion.<br>**d.** Dans le champ **Certificat de signature IDP**, collez le corps du certificat de signature que vous avez téléchargé, y compris les lignes Début du certificat et Fin du certificat.<br><br>Lorsque vous copiez et collez le corps du certificat, veillez à ne pas modifier les sauts de ligne ou le format des informations du certificat.<br>**e.** Dans le champ **ID d'entité SP**, saisissez l'**Identifiant (ID d'entité)** utilisé dans la configuration SAML sur le portail Entra. Ce champ est requis. La valeur « ID d'entité SP » doit correspondre à la valeur « Identifiant (ID d'entité) » que vous avez enregistrée dans la console IDP.<br>**f.** Activez l'option **Afficher les paramètres avancés**, dans le champ **Revendication d'e-mail**, collez la valeur du « Nom de la revendication » que vous avez enregistré sur le portail Entra (par exemple, http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress).<br>**g.** Spécifiez tout autre paramètre facultatif.<br>**h.** Cliquez sur **Enregistrer**.<br>**i.** Ouvrez l'authentificateur que vous avez ajouté. Enregistrez l'**URL de rappel SSO**. Cette URL sera requise dans le champ Portail Entra > Configuration SAML de base > URL de réponse (URL de l'abonné d'assertions). |

| Élément | Description |
| --- | --- |
| Personnalisé (SAML) | Sélectionnez cette option si vous souhaitez que les utilisateurs saisissent des informations d'identification personnalisées sur la page d'ouverture de session principale et activent l'accès initié par IDP à la console Cylance.<br><br>Pour obtenir une description détaillée des étapes de configuration de votre Personnalisé (SAML), reportez-vous aux sections suivantes :<br><br>• Configurer un nouveau Personnalisé (SAML) : Configurer l'authentificateur Personnalisé (SAML) pour une authentification améliorée<br>• Activer l'accès initié par personnalisé pour un Personnalisé (SAML) : Mettre à jour l'authentificateur Personnalisé (SAML) pour activer l'accès initié par IDP à la console Cylance<br><br>**Remarque :** L'URL de rappel SSO au format https://login.eid.blackberry.com/_/resume/saml20/*hash*> est générée lorsque vous enregistrez l'authentificateur.<br><br>**a.** Saisissez un nom pour l'authentificateur.<br>**b.** Si vous souhaitez que les utilisateurs valident leur adresse e-mail avec un code à usage unique lors de leur première connexion, activez **Validation requise**.<br>**c.** Dans le champ **URL de demande de connexion**, saisissez l'URL d'authentification unique du fournisseur d'identité.<br>**d.** Dans le champ **Certificat de signature IDP**, collez le corps du certificat de signature que vous avez téléchargé, y compris les lignes Début du certificat et Fin du certificat.<br><br>Lorsque vous copiez et collez le corps du certificat, veillez à ne pas modifier les sauts de ligne ou le format des informations du certificat.<br>**e.** Dans le champ **ID d'entité SP**, saisissez l'« URI d'audience (ID d'entité SP) » que vous avez enregistrée dans le portail IDP personnalisé. Ce champ est requis. La valeur « ID d'entité SP » doit correspondre à la valeur « URI d'audience (ID d'entité SP) » que vous avez enregistrée dans la console IDP.<br>**f.** Dans le champ **format de l'ID de nom**, spécifiez le format de l'identifiant de nom à demander à l'IDP (par exemple, urn:oasis:names:tc:SAML:1,1:nameid-format:emailAddress).<br>**g.** Dans le champ **Revendication d'e-mail**, saisissez `NameID`. Cette valeur doit correspondre au « format NameID » que vous avez spécifié dans la console IDP. L'adresse e-mail garantit que le bon utilisateur se connecte à la console de gestion.<br>**h.** Spécifiez tout autre paramètre facultatif.<br>**i.** Cliquez sur **Enregistrer**.<br>**j.** Ouvrez l'authentificateur que vous avez ajouté. Enregistrez l'**URL d'authentification unique**. Cette URL sera ajoutée à l'IDP personnalisé. |

| Élément | Description |
| --- | --- |
| Mot de passe administrateur Cylance | Sélectionnez cette option si vous souhaitez que les utilisateurs saisissent leurs informations d'identification de console Cylance. Procédez comme suit :<br>**a.** Saisissez un nom pour l'authentificateur.<br>**b.** Cliquez sur **Enregistrer**. |
| Refuser l'authentification | Sélectionnez cette option si vous souhaitez utiliser une stratégie d'authentification pour empêcher les utilisateurs ou les groupes d'utilisateurs d'accéder à la console Cylance ou à un autre service. Vous pouvez ajouter une autre stratégie ou une exception d'application pour autoriser l'accès à un sous-ensemble d'utilisateurs.<br>**a.** Saisissez un nom pour l'authentificateur.<br>**b.** Cliquez sur **Enregistrer**. |
| Duo MFA | Sélectionnez cette option si vous souhaitez que les utilisateurs s'authentifient à l'aide de l'authentification multifactorielle Duo.<br>Avant d'ajouter Duo en tant qu'authentificateur, vous devez créer une application d'API d'authentification. Pour obtenir des instructions, consultez les informations de Duo.<br>Procédez comme suit :<br>**a.** Saisissez un nom pour l'authentificateur.<br>**b.** Dans la section **Configuration DUO MFA**, saisissez le nom d'hôte de l'API, la clé d'intégration et la clé secrète. Vous trouverez ces informations dans l'onglet Applications du compte Duo de votre organisation. Pour plus d'informations, consultez la documentation Duo. |
| Enterprise | Sélectionnez cette option si vous souhaitez que les utilisateurs s'authentifient à l'aide de leurs informations d'identification pour Active Directory, LDAP ou *my*Account. Les informations d'identification qu'un utilisateur utilisera dépendent du type de compte qui est la source de son compte utilisateur dans la console. Procédez comme suit :<br>**a.** Saisissez un nom pour l'authentificateur.<br>**b.** Cliquez sur **Enregistrer**. |

| Élément | Description |
| --- | --- |
| FIDO | Sélectionnez cette option si vous souhaitez que les utilisateurs enregistrent un terminal FIDO2 et l'utilisent pour vérifier leur identité. Les types de terminaux pris en charge incluent les smartphones, les clés de sécurité USB ou Windows Hello.<br>**a.** Saisissez un nom pour l'authentificateur.<br>**b.** Cliquez sur **Enregistrer**.<br>Lorsque FIDO est le premier facteur d'authentification et qu'un utilisateur enregistre un terminal pour la première fois, un mot de passe à usage unique est également envoyé à l'adresse e-mail qu'il utilise pour se connecter. Lorsque FIDO est utilisé comme deuxième facteur dans une stratégie, un mot de passe à usage unique n'est pas requis lorsqu'un utilisateur enregistre un terminal pour la première fois.<br>Pour plus d'informations sur la suppression des terminaux enregistrés d'un compte d'utilisateur, reportez-vous à la section Supprimer un terminal FIDO enregistré pour un compte utilisateur dans le contenu relatif à l'administration. |
| Annuaire intégré (Active Directory/Entra ID/LDAP) | Sélectionnez cette option si vous souhaitez que les utilisateurs saisissent leur mot de passe Active Directory. Si vous sélectionnez cette option, votre locataire Cylance Endpoint Security doit disposer d'une connexion à l'instance de l'annuaire de l'entreprise. Pour plus d'informations, reportez-vous à Association à votre annuaire d'entreprise. Procédez comme suit :<br>**a.** Saisissez un nom pour l'authentificateur.<br>**b.** Cliquez sur **Enregistrer**. |
| Adresse IP | Sélectionnez cette option si vous souhaitez restreindre l'accès des utilisateurs en fonction de leur adresse IP. Vous pouvez créer plusieurs authentificateurs d'adresses IP et les utiliser pour gérer l'accès de différents groupes, mais vous ne pouvez attribuer qu'un seul authentificateur d'adresses IP par stratégie.<br>Pour obtenir des instructions détaillées sur les étapes pour ajouter ou supprimer des restrictions d'adresses IP pour la console, reportez-vous à la section Ajouter un authentificateur de restriction d'adresse IP pour la console Cylance.<br>**a.** Saisissez un nom pour l'authentificateur.<br>**b.** Dans le champ **Plages d'adresses IP**, spécifiez une ou plusieurs adresses IP, plages IP ou CIDR. Séparez les entrées par une virgule. Par exemple, plage d'adresses IP : 192.168.0.100-192.168.1.255 ou CIDR : 192.168.0.10/24.<br>**c.** Cliquez sur **Enregistrer**. |

| Élément | Description |
| --- | --- |
| Compte local | Sélectionnez cette option si vous souhaitez que les utilisateurs saisissent leurs informations d'identification BlackBerry Online Account (*my*Account). Procédez comme suit :<br>**a.** Saisissez un nom pour l'authentificateur.<br>**b.** Cliquez sur **Enregistrer**. |
| Okta MFA | Sélectionnez cette option si vous souhaitez que les utilisateurs s'authentifient à l'aide de Okta. Procédez comme suit :<br>**a.** Saisissez un nom pour l'authentificateur.<br>**b.** Dans la section **Configuration Okta MFA**, saisissez la clé d'API d'authentification et le domaine d'authentification.<br>**c.** Cliquez sur **Enregistrer**. |
| Okta (OIDC) | Sélectionnez cette option si vous souhaitez que les utilisateurs s'authentifient à l'aide de Okta. Procédez comme suit :<br>**a.** Dans la liste déroulante située sous **Okta**, sélectionnez **OIDC**.<br>**b.** Saisissez un nom pour l'authentificateur.<br>**c.** Dans la section **Client du fournisseur d'identité**, saisissez l'URL du document de découverte OIDC, l'ID du client et la clé privée JWKS.<br>**d.** Cliquez sur **Enregistrer**. |

| Élément | Description |
| --- | --- |
| Okta (SAML) | Sélectionnez cette option si vous souhaitez que les utilisateurs saisissent leurs informations d'identification Okta sur la page d'ouverture de session principale et activent l'accès initié par IDP à la console Cylance.<br><br>Pour connaître les étapes de configuration de votre Okta (SAML), reportez-vous aux sections suivantes :<br><br>• Configurer un nouveau Okta (SAML) : Configurer l'authentificateur Okta (SAML) pour une authentification améliorée<br>• Activer l'accès initié par Okta pour un Okta existant (SAML) : Mettre à jour l'authentificateur Okta (SAML) pour activer l'accès initié par IDP à la console Cylance<br><br>**Remarque :** L'URL de rappel SSO au format https://login.eid.blackberry.com/_/resume/saml20/*hash*> est générée lorsque vous enregistrez l'authentificateur.<br><br>**a.** Dans la liste déroulante située sous **Okta**, sélectionnez **SAML**.<br>**b.** Saisissez un nom pour l'authentificateur.<br>**c.** Si vous souhaitez que les utilisateurs valident leur adresse e-mail avec un code à usage unique lors de leur première connexion, activez **Validation requise**.<br>**d.** Dans le champ **URL de demande de connexion**, saisissez l'URL d'authentification unique du fournisseur d'identité.<br>**e.** Dans le champ **Certificat de signature IDP**, collez le corps du certificat de signature que vous avez téléchargé, y compris les lignes Début du certificat et Fin du certificat.<br><br>Lorsque vous copiez et collez le corps du certificat, veillez à ne pas modifier les sauts de ligne ou le format des informations du certificat.<br>**f.** Dans le champ **ID d'entité SP**, saisissez l'« URI d'audience (ID d'entité SP) » que vous avez enregistrée sur le portail Okta. Ce champ est requis. La valeur « ID d'entité SP » doit correspondre à la valeur « URI d'audience (ID d'entité SP) » que vous avez enregistrée dans la console IDP.<br>**g.** Dans le champ **ID d'entité IDP**, collez l'« émetteur du fournisseur d'identité » que vous avez enregistré à partir de Okta.<br>**h.** Dans le champ **Format de l'identifiant de nom**, sélectionnez le format NameID que vous avez spécifié dans le système Okta (par exemple, urn:oasis:names:tc:SAML:2,0:nameID-format:persistent).<br>**i.** Dans le champ **Revendication d'e-mail**, saisissez `Email`. Cela doit correspondre au nom « Attribut » que vous avez configuré dans la console Okta. L'adresse e-mail garantit que le bon utilisateur se connecte à la console de gestion.<br>**j.** Spécifiez tout autre paramètre facultatif.<br>**k.** Cliquez sur **Enregistrer**.<br>**l.** Ouvrez l'authentificateur que vous avez ajouté. Enregistrez l'URL d'authentification unique. Cette URL sera ajoutée aux champs suivants dans la console Okta > écran Paramètres SAML.<br><br>• URL d'authentification unique<br>• URL SSO à demander |

| Élément | Description |
| --- | --- |
| OneLogin (OIDC) | Sélectionnez cette option si vous souhaitez que les utilisateurs s'authentifient à l'aide de OneLogin. Procédez comme suit :<br>**a.** Dans la liste déroulante située sous **OneLogin**, sélectionnez **OIDC**.<br>**b.** Saisissez un nom pour l'authentificateur.<br>**c.** Si vous souhaitez que les utilisateurs valident leur adresse e-mail avec un code à usage unique lors de leur première connexion, activez **Validation requise**.<br>**d.** Dans la section **Configuration OneLogin**, saisissez l'URL du document de découverte OIDC, l'ID client, le secret de client et la méthode d'authentification.<br>**e.** Cliquez sur **Enregistrer**. |

| Élément | Description |
| --- | --- |
| OneLogin (SAML) | Sélectionnez cette option si vous souhaitez que les utilisateurs saisissent leurs informations d'identification OneLogin sur la page d'ouverture de session principale et activent l'accès initié par IDP à la console Cylance.<br><br>Pour connaître les étapes de configuration de votre OneLogin (SAML), reportez-vous aux sections suivantes :<br><br>• Configurer un nouveau OneLogin (SAML) : Configurer l'authentificateur OneLogin (SAML) pour une authentification améliorée<br>• Activer l'accès initié par OneLogin pour un OneLogin existant (SAML) : Mettre à jour l'authentificateur OneLogin (SAML) pour activer l'accès initié par IDP à la console Cylance<br><br>**Remarque :** L'URL de rappel SSO au format https://login.eid.blackberry.com/_/resume/saml20/*hash*> est générée lorsque vous enregistrez l'authentificateur.<br><br>**a.** Saisissez un nom pour l'authentificateur.<br>**b.** Si vous souhaitez que les utilisateurs valident leur adresse e-mail avec un code à usage unique lors de leur première connexion, activez **Validation requise**.<br>**c.** Dans le champ **URL de demande de connexion**, saisissez l'URL d'authentification unique du fournisseur d'identité.<br>**d.** Dans le champ **Certificat de signature IDP**, collez le corps du certificat de signature que vous avez téléchargé, y compris les lignes Début du certificat et Fin du certificat.<br><br>Lorsque vous copiez et collez le corps du certificat, veillez à ne pas modifier les sauts de ligne ou le format des informations du certificat.<br>**e.** Dans le champ **ID d'entité SP**, saisissez l'« Identifiant (ID d'entité) » enregistré dans la console OneLogin. Ce champ est requis. La valeur « ID d'entité SP » doit correspondre à la valeur « Identifiant (ID d'entité) » que vous avez enregistrée dans la console IDP.<br>**f.** Spécifiez tout autre paramètre facultatif.<br>**g.** Cliquez sur **Enregistrer**.<br>**h.** Ouvrez l'authentificateur que vous avez ajouté. Enregistrez l'URL d'authentification unique. Cette URL sera ajoutée aux champs suivants dans la console OneLogin :<br><br>• Validateur d'URL ACS (abonné)*<br>• URL ACS (abonné)*<br>• URL de déconnexion unique |

| Élément | Description |
| --- | --- |
| Password à usage unique | Sélectionnez cette option si vous souhaitez que les utilisateurs saisissent un mot de passe à usage unique en plus d'un autre type d'authentification.<br><br>**Remarque :** Si vous sélectionnez cette option, vous devez également ajouter un autre authentificateur à votre stratégie d'authentification et le classer plus haut que le mot de passe à usage unique.<br><br>Pour connaître les étapes d'ajout et de suppression de l'authentification par mot de passe à usage unique pour les administrateurs, reportez-vous aux sections suivantes :<br><br>• Ajouter une authentification par mot de passe à usage unique pour les administrateurs<br>• Supprimer l'authentification par mot de passe à usage unique pour les administrateurs<br><br>Procédez comme suit :<br><br>**a.** Saisissez un nom pour l'authentificateur.<br>**b.** Dans la section **Configuration du mot de passe à usage unique**, dans la première liste déroulante, sélectionnez un certain nombre d'intervalles dans la liste déroulante. Tout code dans la fenêtre est valide s'il précède ou suit le code attendu par le nombre d'intervalles d'actualisation que vous spécifiez. L'intervalle d'actualisation est de 30 secondes et le paramètre par défaut est 0.<br>**c.** Dans la section **Configuration du mot de passe à usage unique**, dans la deuxième liste déroulante, indiquez le nombre de fois où les utilisateurs peuvent ignorer la configuration de l'application OTP et s'authentifier sans saisir de code. |
| Ping Identity (OIDC) | Sélectionnez cette option si vous souhaitez que les utilisateurs s'authentifient à l'aide de Ping Identity. Procédez ainsi :<br><br>**a.** Dans la liste déroulante située sous **Ping**, sélectionnez **OIDC**.<br>**b.** Saisissez un nom pour l'authentificateur.<br>**c.** Dans la section **Client du fournisseur d'identité**, saisissez l'URL du document de découverte OIDC, l'ID du client et la clé privée JWKS.<br>**d.** Dans la liste déroulante **Algorithme de signature du jeton d'ID**, sélectionnez l'un des algorithmes de connexion.<br>**e.** Cliquez sur **Enregistrer**. |

| Élément | Description |
| --- | --- |
| Ping Identity (SAML) | Sélectionnez cette option si vous souhaitez que les utilisateurs saisissent leurs informations d'identification Ping Identity sur la page d'ouverture de session principale et activent l'accès initié par IDP à la console Cylance.<br><br>Pour connaître les étapes de configuration de votre Ping Identity (SAML), reportez-vous aux sections suivantes :<br><br>• Configurer un nouveau Ping Identity (SAML) : Configurer l'authentificateur Ping Identity (SAML) pour une authentification améliorée<br>• Activer l'accès initié par Ping Identity pour un OneLogin existant (SAML) : Mettre à jour l'authentificateur Ping Identity (SAML) pour activer l'accès initié par IDP à la console Cylance<br><br>**Remarque :** L'URL de rappel SSO au format https://login.eid.blackberry.com/_/resume/saml20/*hash*> est générée lorsque vous ajoutez l'authentificateur.<br><br>**a.** Dans la liste déroulante située sous **Identité Ping**, sélectionnez **SAML**.<br>**b.** Saisissez un nom pour l'authentificateur.<br>**c.** Si vous souhaitez que les utilisateurs valident leur adresse e-mail avec un code à usage unique lors de leur première connexion, activez **Validation requise**.<br>**d.** Dans le champ **URL de demande de connexion**, saisissez l'URL d'authentification unique du fournisseur d'identité.<br>**e.** Dans le champ **Certificat de signature IDP**, collez le corps du certificat de signature que vous avez téléchargé, y compris les lignes Début du certificat et Fin du certificat.<br><br>Lorsque vous copiez et collez le corps du certificat, veillez à ne pas modifier les sauts de ligne ou le format des informations du certificat.<br>**f.** Dans le champ **ID d'entité SP**, saisissez l'«ID d'entité » enregistré dans la console OneLogin. Ce champ est requis. La valeur « ID d'entité SP » doit correspondre à la valeur «ID d'entité » que vous avez enregistrée dans la console IDP.<br>**g.** Spécifiez tout autre paramètre facultatif.<br>**h.** Cliquez sur **Enregistrer**.<br>**i.** Ouvrez l'authentificateur que vous avez ajouté. Enregistrez l'URL d'**authentification unique**. Cette URL sera requise dans les champs suivants de l'écran Configuration de la console PingOne :<br><br>• Service d'abonné d'assertions (ACS)<br>• URL de l'application |

4. Cliquez sur **Enregistrer**.

**À la fin :** Créer une stratégie d'authentification.

### Considérations relatives à l'ajout d'authentificateurs SAML

Lorsque vous ajoutez un authentificateur SAML, les valeurs d'URL de demande de connexion et de certificat de signature IDP sont requises. Vous devez tenir compte des éléments suivants concernant les champs facultatifs.

**Remarque :** Lorsque vous configurez un fournisseur d'identité externe, vous devez ajouter l'URL de demande de connexion de Cylance Endpoint Security. L'URL doit être au format https://login.eid.blackberry.com/_/resume/saml20/<*hash*>. Les configurations SAML externes prenant en charge une liste d'URL d'authentification unique ou de réponse de service d'abonné d'assertions, dans les configurations existantes, vous pouvez ajouter la nouvelle URL ou celle que vous venez de générer à la liste en tant qu'option secondaire ou remplacer l'URL d'origine. Si vous avez créé votre authentificateur avant décembre 2023 et que vous souhaitez que les utilisateurs accèdent à la console Cylance à l'aide de l'authentification unique, vous devez générer une URL de demande de connexion mise à jour. Pour plus d'informations sur la mise à jour de votre authentificateur, reportez-vous à Authentification améliorée pour la connexion.

| Élément | Description |
|---|---|
| Format NameID | Vous pouvez utiliser ce champ pour spécifier un format d'identifiant de nom facultatif à demander au fournisseur d'identité. |
| Revendication d'ID fédéré | Vous pouvez utiliser ce champ pour spécifier une valeur de revendication facultative faisant office d'ID fédéré pour lier des comptes entre les systèmes. La valeur par défaut est NameID.<br><br>Si votre IDP est configuré pour renvoyer l'adresse e-mail dans une revendication autre que « NameID », vous devez spécifier la revendication dans ce champ. Vous devez utiliser une valeur unique persistante et immuable dans cette revendication (objectGUID ou UUID, par exemple). Il n'est pas recommandé d'utiliser une valeur qui n'est pas unique ou qui est susceptible de changer (une adresse e-mail, par exemple). Lorsque les utilisateurs se connectent, Cylance Endpoint Security utilise la valeur de revendication d'ID fédéré pour créer un ID unique permettant à l'utilisateur de mapper ses identités dans les deux systèmes.<br><br>La valeur que vous avez spécifiée comme revendication d'ID fédéré ne peut pas être modifiée, car elle est utilisée pour lier un utilisateur dans le fournisseur d'identité externe et Cylance Endpoint Security après sa première connexion. |
| Revendication Active Directory | Vous pouvez utiliser ce champ pour spécifier une valeur de revendication facultative utilisée pour mettre en correspondance les objectGUID Active Directory entre les systèmes pour valider les utilisateurs. |

| Élément | Description |
|---|---|
| Revendication d'e-mail | Vous pouvez utiliser ce champ pour spécifier une valeur de revendication facultative utilisée pour mettre en correspondance les adresses e-mail entre les systèmes. La valeur par défaut est « emailD ».<br>Cylance Endpoint Security exige que toutes les réponses SAML contiennent l'adresse e-mail complète des utilisateurs et qu'elle corresponde à l'adresse e-mail enregistrée auprès de Cylance Endpoint Security. Si votre IDP est configuré pour renvoyer l'adresse e-mail dans une revendication autre que « email », vous devez spécifier la revendication dans ce champ. Par exemple, si la revendication configurée dans votre IDP s'appelle « emailAddress », vous devez définir « emailAddress » dans le champ Revendication d'e-mail. Si elles ne correspondent pas, les utilisateurs ne peuvent pas se connecter. |
| ID d'entité SP | Vous pouvez utiliser ce champ pour spécifier un ID d'entité de fournisseur de services facultatif à envoyer au fournisseur d'identité (également appelé chaine d'émetteur).<br>Pour les authentificateurs SAML Entra, ce champ est obligatoire et la valeur que vous saisissez doit correspondre à l'identifiant (ID d'entité) de la configuration SAML dans Entra. |
| ID d'entité IDP | Vous pouvez utiliser ce champ pour spécifier un ID d'entité de fournisseur d'identité facultatif (également appelé émetteur IDP). S'il est fourni, l'émetteur IDP sera validé sur toutes les réponses. |
| Dérive d'horloge acceptée | Vous pouvez utiliser ce champ pour spécifier, en millisecondes, la dérive d'horloge acceptable entre le client et le serveur. |
| Algorithme de signature | Vous pouvez utiliser ce champ pour spécifier l'algorithme de signature pour les demandes de signature. |
| Clé privée de signature | Vous pouvez utiliser ce champ pour spécifier, au format PEM, une clé privée facultative utilisée pour signer toutes les demandes sortantes. |

## Migrer des paramètres d'authentification personnalisés vers la liste des authentificateurs

Vous pouvez migrer vos authentificateurs SAML existants vers la liste des authentificateurs dans Paramètres, afin de les ajouter aux stratégies d'authentification pour les utilisateurs, les groupes ou votre locataire. Lorsque vous migrez les authentificateurs, vous devez mettre à jour l'URL d'authentification unique vers l'URL utilisée par Cylance Endpoint Security. Vous devez également mettre à jour la revendication NameID dans votre configuration IDP externe afin qu'elle renvoie une valeur persistante et immuable au lieu de l'adresse e-mail d'un utilisateur, ou créer une revendication dans le fournisseur d'identité qui peut être utilisé comme revendication d'ID fédéré.

Avant de migrer vos paramètres, en tant que sécurité intégrée, vous devez créer une stratégie d'authentification qui nécessite uniquement le mot de passe de la console Cylance et l'attribuer à un administrateur.

**Remarque :** Lorsque vous migrez les paramètres d'authentification personnalisés, dans le fournisseur d'identité externe, vous devez ajouter l'URL de demande de connexion Cylance Endpoint Security suivante : `https://idp.blackberry.com/_/resume`. Les configurations SAML externes prenant en charge une liste d'URL d'authentification unique ou de réponse de service d'abonné d'assertions, dans les configurations existantes, vous pouvez ajouter la nouvelle URL à la liste en tant qu'option secondaire ou remplacer l'URL d'origine.

Pour en savoir plus sur les authentificateurs SAML, voir Considérations relatives à l'ajout d'authentificateurs SAML.

**Avant de commencer :** Téléchargez un exemplaire du certificat de signature de votre IDP.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres** > **Application**.
2. Dans la section **Authentification personnalisée**, effectuez les opérations suivantes :
   a) Copiez les informations suivantes dans un fichier texte :
      - Nom du fournisseur
      - URL de connexion
   b) Cochez la case **Autoriser la connexion par mot de passe**. Pour plus d'informations sur ce paramètre, consultez Descriptions de l'authentification personnalisée.
3. Dans la barre de menus, cliquez sur **Paramètres** > **Authentification**.
4. Dans l'onglet **Authentificateurs**, cliquez sur **Ajouter un authentificateur**.
5. Dans la liste déroulante **Type d'authentificateur**, cliquez sur l'authentificateur SAML correspondant au fournisseur que vous avez copié à l'étape 2 (Entra ou Okta, par exemple) ou cliquez sur SAML personnalisé.
6. Dans la section **Informations générales**, saisissez le nom de l'authentificateur.
7. Dans la section **Configuration SAML**, si vous souhaitez que les utilisateurs valident leur adresse e-mail avec un code à usage unique lors de leur première connexion, activez **Validation requise**.
8. Dans le champ **URL de demande de connexion**, saisissez l'URL d'authentification unique du fournisseur d'identité.
9. Dans le champ **Certificat de signature IDP**, collez le corps du certificat de signature que vous avez téléchargé, y compris les lignes Début du certificat et Fin du certificat.

   Lorsque vous copiez et collez le corps du certificat, veillez à ne pas modifier les sauts de ligne ou le format des informations du certificat.
10. Effectuez l'une des opérations suivantes :

| Tâche | Étapes |
| --- | --- |
| Mettez à jour les valeurs de revendication NameID et email dans le fournisseur d'identité externe. | **a.** Connectez-vous à votre fournisseur d'identité externe.<br>**b.** Mettez à jour l'URL d'authentification unique de Cylance Endpoint Security en `https://idp.blackberry.com/_/resume`. Vous pouvez ajouter cette URL à l'URL login.<*region*>.cylance.com existante.<br>**c.** Modifiez la revendication NameID afin qu'elle renvoie une valeur persistante et immuable (objectGUID ou UUID, par exemple) qui peut être utilisée dans la revendication d'ID fédéré au lieu de l'adresse e-mail de l'utilisateur. Pour obtenir des instructions, reportez-vous à la documentation du fournisseur d'identité.<br>**d.** Créez une revendication email qui renverra l'adresse e-mail de l'utilisateur. |

| Tâche | Étapes |
| --- | --- |
| Créez une revendication dans votre fournisseur d'identité externe et ajoutez-la aux paramètres de l'authentificateur. | **a.** Connectez-vous à votre fournisseur d'identité externe.<br>**b.** Mettez à jour l'URL d'authentification unique de Cylance Endpoint Security en `https://idp.blackberry.com/_/resume`. Vous pouvez ajouter cette URL à l'URL login.<*region*>.cylance.com existante.<br>**c.** Créez une revendication qui renvoie un ID persistant et immuable pour un utilisateur. Pour obtenir des instructions, reportez-vous à la documentation du fournisseur d'identité.<br>**d.** Dans la console de gestion Cylance, dans le champ **Revendication d'e-mail**, saisissez `nameID`. La valeur nameID doit utiliser un « n » minuscule.<br>**e.** Dans le champ **Revendication d'ID fédéré**, saisissez le nom de la revendication que vous venez de créer dans le fournisseur d'identité externe. |

**11.**Cliquez sur **Enregistrer**.

**À la fin :**

- Créer une stratégie d'authentification.
- En cas de problème de connexion à l'aide de l'authentificateur SAML dans le cadre d'une stratégie d'authentification, vous pouvez télécharger un exemple de réponse SAML à partir de votre IDP et valider les noms des revendications.

# Gérer les stratégies d'authentification pour votre locataire

Par défaut, Cylance Endpoint Security possède trois stratégies d'authentification des locataires qui sont utilisées pour gérer les types d'authentification que les administrateurs doivent effectuer pour se connecter à la console Cylance et que les utilisateurs doivent effectuer pour activer les applications ou agents de Cylance Endpoint Security (par exemple, l'application CylancePROTECT Mobile ou CylanceGATEWAY). Les stratégies de locataire sont appliquées lorsqu'aucune exception d'application ou stratégie d'authentification n'est attribuée à l'utilisateur pour la console ou l'application à laquelle il tente d'accéder. Les stratégies par défaut et leurs authentificateurs sont les suivants :

- Console d'administration : cette stratégie utilise le mot de passe de la console de Cylance comme authentificateur par défaut. Pour les locataires créés après mars 2024, cette stratégie utilise le mot de passe de console Cylance et le mot de passe à usage unique comme authentificateurs par défaut. Il est utilisé pour l'authentification à la console de gestion de Cylance Endpoint Security.
- CylanceGATEWAY : cette stratégie utilise le mot de passe d'entreprise de l'utilisateur comme authentificateur par défaut. Il est utilisé lorsque les utilisateurs activent l'application ou l'agent de bureau de CylanceGATEWAY.
- Application CylancePROTECT Mobile : cette stratégie utilise le mot de passe d'entreprise de l'utilisateur comme authentificateur par défaut. Il est utilisé lorsque les utilisateurs activent l'application CylancePROTECT sur des appareils mobiles. Elle n'est pas appliquée lorsque l'utilisateur active l'agent de bureau.

Vous pouvez modifier les stratégies pour ajouter d'autres types d'authentification que les utilisateurs doivent effectuer dans l'ordre que vous spécifiez dans la stratégie. Par exemple, si vous ajoutez Enterprise avant un mot de passe à usage unique, les utilisateurs saisissent leurs informations d'identification *my*Account ou avant de recevoir une invite de mot de passe à usage unique.

**Avant de commencer :** Ajouter un authentificateur.

1. Dans la barre de menus, cliquez sur **Paramètres > Authentification > Authentification par défaut**.

2. Cliquez sur la stratégie que vous voulez modifier.
3. Dans la section **Application d'authentification**, cliquez sur **Ajouter un authentificateur**.
4. Dans la boîte de dialogue **Ajouter un authentificateur**, sélectionnez un authentificateur. Cliquez sur **Ajouter**.

   Répétez cette étape pour ajouter d'autres authentificateurs à la stratégie. Les utilisateurs doivent effectuer les types d'authentification dans l'ordre que vous spécifiez. Pour modifier l'ordre, cliquez sur **Définir l'ordre**, faites glisser les authentificateurs dans l'ordre de votre choix, puis cliquez sur **Définir l'ordre**.

   **Remarque :** Si vous ajoutez un mot de passe à usage unique en tant qu'authentificateur, il doit être défini après le mot de passe d'entreprise

   encore une fois.
5. Cliquez sur **Enregistrer**.

Si vous ajoutez des authentificateurs à une stratégie par défaut, vous pouvez cliquer sur rétablir la méthode par défaut sur la page liste des stratégies pour restaurer le paramètre par défaut.

# Créer une stratégie d'authentification

Vous créez une politique d'authentification pour spécifier les types d'authentification que les administrateurs doivent effectuer pour se connecter à la console de gestion de Cylance Endpoint Security et que les utilisateurs doivent compléter pour activer les applications ou agents Cylance Endpoint Security (par exemple, CylancePROTECT Mobile ou CylanceGATEWAY) . Les utilisateurs doivent effectuer les types d'authentification dans l'ordre que vous spécifiez dans la stratégie. Par exemple, si vous ajoutez Enterprise avant un mot de passe à usage unique, les utilisateurs saisissent leurs informations d'identification *my*Account ou professionnelles avant de recevoir une invite de mot de passe à usage unique.

Dans une stratégie, vous pouvez également configurer des exceptions d'application et spécifier différents authentificateurs pour des applications spécifiques. Les exceptions d'application sont prioritaires sur la stratégie d'authentification. Toutes les stratégies d'authentification configurées dans votre locataire sont appliquées dans l'ordre suivant :

1. Exceptions d'application dans les stratégies d'authentification attribuées aux utilisateurs ou aux groupes
2. Stratégies d'authentification attribuées à des utilisateurs ou des groupes
3. Stratégie d'authentification des locataires

**Avant de commencer :** Ajouter un authentificateur

1. Sur la barre de menus, cliquez sur **Stratégies > Stratégie d'utilisateur**.
2. Cliquez sur l'onglet **Authentification**.
3. Cliquez sur **Ajouter une stratégie**.
4. Saisissez le nom et la description de la stratégie.
5. Dans la section **Règles d'authentification**, cliquez sur **Ajouter un authentificateur**.

   Si votre authentificateur a été créé avant décembre 2023, et si vous avez mis à jour l'URL de demande de connexion à Cylance Endpoint Security afin que le proxy initié par IDP permette aux utilisateurs d'utiliser l'authentification unique (SSO) pour accéder à la console Cylance après s'être connectés au portail IDP de leurs utilisateurs, ajoutez l'authentificateur mis à jour et supprimez l'authentification d'origine qui a été créée. Pour plus d'informations, reportez-vous à Authentification améliorée pour la connexion.
6. Dans la boite de dialogue **Ajouter un authentificateur**, sélectionnez un authentificateur du menu déroulant.

   Répétez cette étape pour ajouter d'autres authentificateurs à la stratégie. Les utilisateurs reçoivent des invites de chaque authentificateur dans l'ordre dans lequel ils sont répertoriés dans la stratégie. Si vous ajoutez Duo MFA à la stratégie, vous devez également ajouter un autre authentificateur afin d'utiliser Duo comme second facteur d'authentification. Pour modifier l'ordre, cliquez sur **Définir l'ordre**, faites glisser les authentificateurs dans l'ordre de votre choix, puis cliquez à nouveau sur **Définir l'ordre**.

7. Si vous souhaitez ajouter des exceptions d'application, cliquez sur **Gérer les exceptions d'application**.
8. Dans la boite de dialogue **Gérer les exceptions d'application**, sélectionnez les applications que vous souhaitez inclure dans le volet **Applications disponibles**.
9. Cliquez sur >.
10. Cliquez sur **Enregistrer**.
11. Dans la section **Gérer les exceptions d'application**, cliquez sur l'onglet de l'une des applications que vous avez ajoutées en tant qu'exception.
12. Cliquez sur **Ajouter un authentificateur**.
13. Dans la boite de dialogue **Ajouter un authentificateur**, sélectionnez un authentificateur du menu déroulant. Cliquez sur **Enregistrer**.

    Répétez cette étape pour ajouter d'autres authentificateurs aux exceptions d'applications. Les utilisateurs doivent effectuer les types d'authentification dans l'ordre que vous spécifiez. Pour modifier l'ordre, cliquez sur **Définir l'ordre**, faites glisser les authentificateurs dans l'ordre de votre choix, puis cliquez à nouveau sur **Définir l'ordre**.
14. Pour enregistrer la stratégie, cliquez sur **Enregistrer**.

**À la fin :** Attribuer des stratégies à des administrateurs, des utilisateurs et des groupes.

# Attribuer des stratégies à des administrateurs, des utilisateurs et des groupes

Vous pouvez attribuer des stratégies d'utilisateur à un nombre illimité de groupes, d'administrateurs et d'utilisateurs, mais chaque administrateur et chaque utilisateur ne peut avoir qu'une seule stratégie d'utilisateur de chaque type qui lui est attribuée. Une stratégie attribuée directement à un utilisateur ou un administrateur est prioritaire sur les stratégies attribuées à des groupes auxquels il appartient. Si aucune stratégie n'est attribuée directement à un utilisateur ou un administrateur et que celui-ci appartient à au moins deux groupes auxquels différentes stratégies de type identique sont attribuées, la stratégie attribuée la mieux classée est appliquée à l'utilisateur ou l'administrateur.

Chaque connexion à la console de gestion est évaluée par rapport aux stratégies attribuées aux administrateurs et aux utilisateurs, dans l'ordre, jusqu'à ce qu'une stratégie qui lui est attribuée corresponde. Si aucune stratégie n'est attribuée directement à l'administrateur ou à l'utilisateur, ou par l'intermédiaire d'un groupe dont il est membre, la stratégie par défaut est appliquée et il ne peut se connecter à la console Cylance qu'à l'aide de son mot de passe Cylance. Les stratégies d'authentification améliorées sont appliquées aux administrateurs et aux utilisateurs dans l'ordre suivant :

- Exceptions de l'application de stratégie d'utilisateur
- Stratégie d'utilisateur
- Stratégie d'application de locataire
- Stratégie par défaut

**Avant de commencer :** Si les types de stratégie suivants sont utilisés, créez-en une ou plusieurs :

- Stratégie d'inscription
- Stratégie CylancePROTECT Mobile
- Stratégie de service CylanceGATEWAY
- Stratégie d'authentification

1. Sur la barre de menus, cliquez sur **Stratégies > Stratégie d'utilisateur**.
2. Sélectionnez l'onglet correspondant au type de stratégie que vous souhaitez attribuer.
3. Cliquez sur le nom de la stratégie que vous souhaitez attribuer.

4. Cliquez **Groupes et utilisateurs attribués**.
5. Cliquez sur **Ajouter un utilisateur ou un groupe**.
6. Cliquez sur l'onglet **Utilisateur**.
7. Commencez à saisir un nom pour rechercher l'utilisateur. Par défaut, 50 résultats de recherche maximum sont renvoyés. Affinez votre recherche lorsque plus de 50 résultats de recherche sont renvoyés.

   Les comptes administrateur sont affichés avec une icône dans la liste des utilisateurs. Dans certains scénarios, vous pouvez voir deux comptes utilisateur pour un utilisateur, un compte administrateur et un compte utilisateur Active Directory.
8. Sélectionnez un ou plusieurs noms dans les résultats de la recherche. Cliquez sur **Ajouter**.

   Vous pouvez également attribuer des stratégies à un utilisateur sur la page de configuration utilisateur.
9. Cliquez sur l'onglet **Groupe d'utilisateurs**.
10. Commencez à saisir un nom pour rechercher le groupe que vous souhaitez ajouter. Par défaut, 50 résultats de recherche maximum sont renvoyés. Affinez votre recherche lorsque plus de 50 résultats de recherche sont renvoyés.
11. Sélectionnez un ou plusieurs noms dans les résultats de la recherche. Cliquez sur **Ajouter**.

    Vous pouvez attribuer des stratégies à un groupe à partir de la page des paramètres de groupe.
12. Pour annuler l'attribution de la stratégie à un utilisateur ou à un groupe, sélectionnez les utilisateurs et les groupes concernés, puis cliquez sur **Supprimer**.

## Classer les stratégies

Vous pouvez attribuer des stratégies à des utilisateurs individuels et à des groupes d'utilisateurs. La stratégie que vous attribuez à un utilisateur individuel est prioritaire sur les stratégies attribuées aux groupes auxquels appartient l'utilisateur. Si aucune stratégie n'est attribuée directement à un utilisateur et que l'utilisateur appartient à deux groupes ou plus auxquels des stratégies différentes sont attribuées, la stratégie attribuée ayant le classement le plus élevé est appliquée à l'utilisateur.

Avant de classer les stratégies, vous devez décider d'une stratégie en fonction de vos objectifs et des groupes auxquels vous attribuez les stratégies. Par exemple, vous voulez peut-être que les stratégies de contrôle d'accès réseau s'appliquant à des groupes de services spécifiques soient classées au plus haut niveau et que les stratégies les plus restrictives soient classées en dessous, ou vous souhaitez que la stratégie la plus restrictive soit classée en tête.

1. Sur la barre de menus, cliquez sur **Stratégies > Stratégie d'utilisateur**.
2. Sélectionnez l'onglet correspondant au type de stratégie que vous souhaitez attribuer.
3. Cliquez sur **Classer**.
4. Pour modifier le classement d'une stratégie dans la liste, faites glisser l'icône pour la stratégie vers une nouvelle position dans la liste.
5. Cliquez sur **Enregistrer**.

# Inscription de CylancePROTECT Mobile et des utilisateurs CylanceGATEWAY

Vous attribuez une stratégie d'inscription aux utilisateurs pour leur permettre d'activer l'application CylancePROTECT Mobile sur les terminaux mobiles et les agents CylanceGATEWAY sur les terminaux Windows et macOS.

La stratégie d'inscription inclut des paramètres distincts pour les terminaux mobiles et de bureau. Vous pouvez spécifier les types de terminaux pris en charge et le texte des e-mails à envoyer aux utilisateurs pour fournir des instructions d'activation, ainsi qu'un mot de passe ou QR Code requis pour commencer le processus d'activation. Vous pouvez spécifier le nombre de jours pendant lesquels le mot de passe d'activation ou QR Code est valide sous **Paramètres > Activation**. Le paramètre s'applique à toutes les stratégies d'inscription.

Les stratégies suivantes doivent être attribuées aux utilisateurs avant de pouvoir activer l'application CylancePROTECT Mobile ou l'agent CylanceGATEWAY.

| Type d'utilisateur | Stratégies requises |
| --- | --- |
| Utilisateur de l'application CylancePROTECT Mobile sans prise en charge de CylanceGATEWAY | • Stratégie d'inscription<br>• CylancePROTECT Mobile stratégie |
| Utilisateur de l'application CylancePROTECT Mobile avec prise en charge uniquement de CylanceGATEWAY | • Stratégie d'inscription<br>• Stratégie de service Gateway |
| Utilisateur de l'application CylancePROTECT Mobile avec prise en charge de CylancePROTECT Mobile et de CylanceGATEWAY | • Stratégie d'inscription<br>• CylancePROTECT Mobile stratégie<br>• Stratégie de service Gateway |
| Utilisateur de bureau avec l'agent CylanceGATEWAY | • Stratégie d'inscription<br>• Stratégie de service Gateway |

**Remarque :** L'agent CylanceGATEWAY communique avec la console de gestion via des Websockets sécurisés (WSS) et doit être en mesure d'établir cette connexion directement. Vous devez configurer le réseau de votre organisation pour autoriser les connexions aux domaines appropriés. Par exemple, pour permettre à l'agent CylanceGATEWAY de s'activer et de s'authentifier régulièrement, vous devez autoriser l'accès à idp.blackberry.com et au domaine de votre région. Si votre environnement utilise un proxy d'authentification, vous devez autoriser le trafic sur le serveur proxy. Si les domaines appropriés ne sont pas autorisés, l'agent CylanceGATEWAY ne parvient pas à ouvrir le navigateur pour terminer le processus d'authentification. Pour en savoir plus sur les ports devant être ouverts pour CylanceGATEWAY, rendez-vous sur le site support.blackberry.com/community pour consulter l'article 79017. Pour en savoir plus sur la configuration réseau requise pour Cylance Endpoint Security, consultez la section Configuration réseau requise pour Cylance Endpoint Security.

## Créer une stratégie d'inscription

1. Sur la barre de menus de la console de gestion, cliquez sur **Stratégies > Stratégie utilisateur**.
2. Cliquez sur l'onglet **Inscription**.

3. Cliquez sur l'onglet **Ajouter une stratégie**.
4. Saisissez le nom et la description de la stratégie.
5. Pour définir des options d'inscription pour les utilisateurs de terminaux mobiles avec l'application CylancePROTECT Mobile, procédez comme suit :
   a) Cliquez sur **Mobile**.
   b) Pour limiter les types de terminaux que l'utilisateur peut inscrire, sous **Plateformes autorisées**, désactivez **iOS** ou **Android**.
   c) Sous **Courrier électronique de bienvenue UES Mobile**, consultez l'objet du message électronique envoyé aux utilisateurs et mettez-le à jour si nécessaire.
   d) Mettez à jour le corps du message si nécessaire pour fournir des informations propres à votre organisation.

      Vous pouvez utiliser des variables dans l'e-mail.
6. Pour définir les options d'inscription de l'agent CylanceGATEWAY sur les terminaux Windows et macOS, procédez comme suit :
   a) Cliquez sur **Gateway Desktop**.
   b) Pour limiter les types de terminaux que l'utilisateur peut inscrire, sous **Plateformes autorisées**, désactivez **Windows** ou **macOS**.
   c) Sous **Courrier électronique de bienvenue**, consultez l'objet de l'e-mail envoyé aux utilisateurs et mettez-le à jour si nécessaire.
   d) Mettez à jour le corps du message si nécessaire pour fournir des informations propres à votre organisation.

      Vous pouvez utiliser des variables dans l'e-mail. Les utilisateurs doivent saisir la valeur {{CustomDomain}} dans le champ Domaine personnalisé de la première page d'ouverture de session. Vous pouvez utiliser la variable pour insérer la valeur ou la rechercher sous **Paramètres > Application** dans le champ **Entreprise**.
7. Cliquez sur **Ajouter**.

**À la fin :** Attribuer la stratégie à des utilisateurs et groupes.

# Variables d'e-mail d'inscription prises en charge

Vous pouvez utiliser les variables suivantes dans le texte du message électronique spécifié par la stratégie d'inscription :

| Variable | Description |
|---|---|
| {{UserDisplayName}} | Nom d'affichage de l'utilisateur tel qu'il apparaît sur la page de l'utilisateur ou dans le répertoire à partir duquel l'utilisateur a été intégré. |
| {{FullUserName}} | Nom complet de l'utilisateur tel qu'il apparaît sur la page de l'utilisateur ou dans le répertoire à partir duquel l'utilisateur a été intégré. |
| {{UserName}} | Nom de l'utilisateur tel qu'il apparaît sur la page de l'utilisateur ou dans le répertoire à partir duquel l'utilisateur a été intégré. |
| {{UserEmailAddress}} | Adresse électronique de l'utilisateur tel qu'elle apparaît sur la page de l'utilisateur ou dans le répertoire à partir duquel l'utilisateur a été intégré. |
| {{CustomDomain}} | Nom de domaine d'entreprise Cylance Endpoint Security de votre organisation. Cette valeur s'affiche sous **Paramètres > Application** dans le champ **Entreprise**. |

| Variable | Description |
| --- | --- |
| {{EnrollmentQRCode}} | Code QR généré par Cylance Endpoint Security pour simplifier l'activation de l'application CylancePROTECT Mobile sur les terminaux mobiles. Cette variable ne peut être utilisée que dans l'e-mail envoyé aux utilisateurs de terminaux mobiles. |
| {{EnrollmentPasscode}} | Mot de passe d'activation généré par Cylance Endpoint Security |
| {{EnrollmentPasscodeExpiry}} | Date d'expiration du mot de passe d'activation et du code QR. Vous pouvez définir le nombre de jours pendant lesquels le mot de passe d'activation ou le code QR est valide sous **Paramètres > Activation**. |

# Configurer les zones pour gérer CylancePROTECT Desktop et CylanceOPTICS

Vous pouvez utiliser des zones pour regrouper et gérer les terminaux CylancePROTECT Desktop et CylanceOPTICS. Vous pouvez regrouper ces terminaux en fonction de la zone géographique (par exemple, l'Asie et l'Europe), de la fonction (par exemple, le personnel des ventes et du service informatique) ou de tout critère requis par votre organisation.

Vous pouvez attribuer une stratégie de terminal à une zone et l'appliquer aux terminaux CylancePROTECT Desktop et CylanceOPTICS dans la zone. Vous pouvez également ajouter une règle de zone qui peut ajouter des terminaux à une zone en fonction de critères spécifiés dans une requête enregistrée, tels que le nom de domaine, la plage d'adresses IP ou le système d'exploitation. Les nouveaux terminaux seront automatiquement ajoutés à une zone s'ils correspondent aux critères de règles de la zone.

Par défaut, les terminaux ajoutés automatiquement à la zone suivent les règles de la zone. Si l'option de suppression automatique du terminal est sélectionnée dans les règles de zone, les terminaux qui suivent les règles de zone seront automatiquement supprimés de la zone lorsqu'ils ne répondent pas aux critères des règles de zone. Vous pouvez également ajouter manuellement des terminaux qui ignorent les règles de zone afin qu'ils ne soient pas automatiquement supprimés de la zone. Lors de la gestion d'une zone, vous pouvez choisir si un appareil suit ou ignore les règles de la zone.

Notez que les utilisateurs administrateurs disposant du rôle Gestionnaire de zone peuvent installer des agents sur les terminaux, mais ils n'ont pas accès à la zone par défaut (non zonée), de sorte qu'ils ne peuvent pas attribuer de terminaux à des zones.

Lorsque vous créez un nouveau locataire Cylance Endpoint Security, ou lorsque vous réinitialisez un locataire à l'état par défaut recommandé, BlackBerry fournit des zones préconfigurées et des stratégies de terminal préconfigurées conçues pour vous aider à adapter votre environnement à la posture de sécurité souhaitée. Pour plus d'informations, reportez-vous à Configuration d'un nouveau locataire Cylance Endpoint Security.

## Ajouter et configurer une zone

**Avant de commencer :** Si vous souhaitez ajouter une règle de zone à la zone, vous devez créer et enregistrer une requête à partir de l'écran Actifs > Terminaux. La liste des terminaux dans les résultats de la requête enregistrée indique les terminaux qui seront automatiquement ajoutés à la zone.

1. Dans la console de gestion, cliquez sur **Zones** sur la barre de menu.
2. Cliquez sur **Ajouter une nouvelle zone**.
3. Dans le champ **Nom de la zone**, saisissez un nom.
4. Dans la liste déroulante **Stratégie**, cliquez sur une stratégie de terminal à associer à la zone.
5. Dans le champ **Valeur**, cliquez sur le niveau de priorité approprié pour la zone. Ce paramètre n'a aucun impact sur la gestion des zones ou des terminaux.
6. Cliquez sur **Enregistrer**.
7. Dans la liste des zones, cliquez sur le nom de la zone que vous avez créée.
8. Effectuez l'une des opérations suivantes :

| Tâche | Étapes |
| --- | --- |
| Ajoutez une règle de zone pour ajouter automatiquement des terminaux. | Vous avez besoin d'une requête enregistrée pour ajouter une règle de zone.<br>**a.** Cliquez sur **Créer une règle**.<br>**b.** Sélectionnez une requête enregistrée. Les paramètres de recherche s'affichent.<br>**c.** Si vous souhaitez appliquer automatiquement la stratégie de terminal associée à la zone, sélectionnez **Appliquer la stratégie de zone aux terminaux lorsqu'ils sont ajoutés à la zone**.<br>**d.** Si vous souhaitez supprimer automatiquement de la zone les terminaux qui ne correspondent pas aux critères de la règle de zone, sélectionnez **Supprimer automatiquement les terminaux de cette zone**. Cela concerne uniquement les terminaux qui suivent les règles de zone.<br>**e.** Cliquez sur **Enregistrer**. |
| Ajoutez manuellement des terminaux à la zone. | Lorsque vous ajoutez manuellement un terminal à une zone, celui-ci ignore les règles de zone par défaut. Un terminal qui ignore les règles de zone restera dans la zone même s'il ne correspond pas aux critères de la règle de zone.<br>**a.** Sous l'onglet **Terminaux**, cliquez sur **Ajouter un terminal à la zone**.<br>**b.** Sélectionnez les terminaux à ajouter. Vous pouvez appliquer des filtres pour rechercher des terminaux.<br>**c.** Si vous souhaitez appliquer de zone aux terminaux sélectionnés, cochez la case **Appliquer la stratégie de zone aux terminaux sélectionnés**.<br>**d.** Cliquez sur **Enregistrer**. |
| Appliquez la stratégie de terminal de zone à tous les utilisateurs de la zone. | Cette action remplace toutes les stratégies de terminal actuellement attribuées aux terminaux par la stratégie de terminal actuellement attribuée à la zone.<br>**a.** Cochez la case **Appliquer à tous les terminaux de cette zone**.<br>**b.** Cliquez sur **Enregistrer**. |
| Définissez un terminal pour qu'il suive ou ignore une règle de zone. | Dans la liste des terminaux d'une zone, les terminaux qui suivent cette règle de zone peuvent être identifiés dans la colonne Règle de zone. Les terminaux qui suivent les règles de la zone sont soumis à un retrait automatique de la zone. Les terminaux qui ignorent les règles de zone resteront dans la zone (sauf si vous les supprimez manuellement).<br>**a.** Dans l'onglet **Terminaux**, sélectionnez un ou plusieurs terminaux.<br>**b.** Cliquez sur **Suivre la règle de zone** ou **Ignorer la règle de zone**.<br>**c.** Cliquez sur **Oui**. |
| Copiez des terminaux dans une autre zone. | **a.** Dans l'onglet **Terminaux**, sélectionnez un ou plusieurs terminaux.<br>**b.** Cliquez sur **Copier un terminal**.<br>**c.** Sélectionnez une ou plusieurs zones.<br>**d.** Cliquez sur **Enregistrer**. |

| Tâche | Étapes |
| --- | --- |
| Supprimez des terminaux d'une zone. | **a.** Dans l'onglet **Terminaux**, sélectionnez un ou plusieurs terminaux.<br>**b.** Cliquez sur **Supprimer le terminal de la zone**.<br>**c.** Cliquez sur **Oui**. |

# Configurer CylancePROTECT Desktop

| Étape | Action |
|---|---|
| 1 | Consultez la configuration requise pour CylancePROTECT Desktop. |
| 2 | Créez et configurez une stratégie de terminal.<br>• Les nouveaux locataires incluent des zones préconfigurées et des stratégies de terminaux qui vous permettent d'adapter plus facilement votre environnement à la stratégie de sécurité souhaitée.<br>• Consultez les recommandations pour la création et le test des stratégies de terminal.<br>• Passez en revue les recommandations pour la gestion de zone. |
| 3 | Installez l'agent CylancePROTECT Desktop sur des terminaux<br>• Installation de l'agent CylancePROTECT Desktop pour Windows<br>• Installation de l'agent CylancePROTECT Desktop pour macOS<br>• Installation de l'agent CylancePROTECT Desktop pour Linux |
| 4 | Gérer les mises à jour pour les agents CylancePROTECT Desktop et CylanceOPTICS. |

# Test de votre déploiement CylancePROTECT Desktop

Avant de déployer l'agent CylancePROTECT Desktop sur les terminaux, vous devez tester son comportement avec d'autres applications dans un environnement de test, afin de vérifier que les applications utilisées dans votre organisation sont autorisées à s'exécuter et à fonctionner comme prévu. Par exemple, si vous découvrez que l'agent empêche certaines applications de s'exécuter correctement, vous pouvez configurer des exclusions pour permettre l'exécution.

Lorsque vous créez un nouveau locataire Cylance Endpoint Security, ou lorsque vous réinitialisez un locataire à l'état par défaut recommandé, BlackBerry fournit des zones préconfigurées et des stratégies de terminal préconfigurées conçues pour vous aider à adapter votre environnement à la posture de sécurité souhaitée. Pour plus d'informations, reportez-vous à Configuration d'un nouveau locataire Cylance Endpoint Security.

Lorsque vous souhaitez tester l'agent, installez-le sur des systèmes de test qui incluent des applications utilisées dans votre organisation, afin de vous assurer qu'il représente précisément l'environnement réel.

Pour tester l'agent, procédez comme suit :

1. Créer des stratégies de test.
2. Créer des zones de test.

Les stratégies de terminal contiennent les paramètres de l'agent et lui indiquent ce qu'il faut faire lorsqu'il rencontre une menace. Les zones vous aident à regrouper vos systèmes par emplacement géographique, unité commerciale, système d'exploitation ou autres propriétés de groupe. Les règles de zone permettent d'attribuer automatiquement des systèmes à une zone en fonction des critères que vous définissez (par exemple, système d'exploitation, plage d'adresses IP et autres critères). Vous devez tester les stratégies et les zones pour vous familiariser avec ces fonctionnalités et pour vous aider à planifier leur utilisation dans votre entreprise.

## Créer une stratégie de test CylancePROTECT Desktop

Vous devez mettre en œuvre des fonctions de stratégie CylancePROTECT Desktop par étapes afin de vous assurer que les performances et les opérations ne sont pas affectées. Par défaut, lorsque vous créez une stratégie de terminal, les fonctions de stratégie ne sont pas activées et vous devez les activer manuellement. À mesure que vous comprenez les types de menaces qui sont consignées dans votre environnement et le comportement de l'agent CylancePROTECT Desktop, vous pouvez activer progressivement davantage de fonctions de stratégie.

Il est recommandé de tester les stratégies sur les terminaux qui incluent les applications utilisées dans votre organisation. Il est important que les terminaux que vous utilisez pour tester les stratégies représentent précisément les terminaux qui se trouvent dans votre environnement de production, et pas seulement une machine propre, afin de garantir que les applications sont autorisées à s'exécuter correctement lorsque les stratégies sont appliquées via l'agent CylancePROTECT Desktop. Par exemple, vous pouvez sélectionner un sous-ensemble de terminaux dans votre environnement de production, qui incluent toutes les applications (propriétaires et personnalisées) dont les utilisateurs ont besoin pour leurs activités quotidiennes.

L'agent utilise le contrôle d'exécution et le contrôle de processus pour analyser uniquement les processus en cours d'exécution. Cela inclut tous les fichiers qui s'exécutent au démarrage, qui sont définis sur exécution automatique et qui sont exécutés manuellement par l'utilisateur. L'agent envoie uniquement des alertes à la console de gestion. Par défaut, aucun fichier n'est bloqué ou mis en quarantaine.

1. Dans la console de gestion, cliquez sur **Stratégies > Stratégie de terminal > Ajouter une nouvelle stratégie**.
2. Dans le champ **Nom de la stratégie**, saisissez le nom de la stratégie de test.
3. Activez le **Chargement automatique** pour analyser et envoyer les fichiers suspects aux services cloud CylancePROTECT pour une analyse plus approfondie.
   a) Dans l'onglet **Actions de fichier**, dans la section **Chargement automatique**, sélectionnez tous les types de fichiers disponibles.
   b) Cliquez sur **Créer** pour créer la stratégie de test initiale.
   c) Attribuez la stratégie de test initiale aux points de terminaison CylancePROTECT Desktop que vous utilisez pour le test.
   d) Autorisez les terminaux auxquels la stratégie de test est attribuée à s'exécuter au moins pendant une journée pour permettre l'exécution et l'analyse des applications et des processus généralement utilisés sur le terminal. Il est possible que vous souhaitiez prendre en compte toutes les applications requises qui s'exécutent périodiquement sur un terminal (par exemple, une fois par semaine) et qui doivent être surveillées en dehors de cette exécution de test.
   e) Lors du test de la stratégie, accédez à l'écran **Protection > Menaces** de la console de gestion pour afficher la liste des applications et processus considérés comme une menace (anormale ou dangereuse) par CylancePROTECT et identifiez ceux qui doivent être autorisés à s'exécuter sur le point de terminaison. Vous pouvez cliquer sur une menace pour afficher plus d'informations à son sujet et télécharger le fichier malveillant pour effectuer votre propre recherche de menace. Le fichier malveillant n'est pas modifié, mais renommé à l'aide du hachage SHA256 sans extension de fichier pour éviter sa détonation accidentelle. Si vous le renommez pour inclure l'extension de fichier d'origine, le fichier malveillant peut être exécuté. Aucune information personnelle n'est partagée avec la console ou avec d'autres locataires ou organisations.
   f) Accédez à **Stratégies > Stratégie de terminal** et modifiez la stratégie de terminal pour permettre l'exécution d'applications et de processus spécifiques sur les points de terminaison auxquels cette stratégie est attribuée. Vous pouvez ajouter des fichiers à la section **Liste sécurisée des stratégies** de l'onglet **Actions de fichier**.

      Vous pouvez également mettre en quarantaine ou supprimer des fichiers sur des terminaux spécifiques ou sur tous les terminaux de votre organisation. Pour plus d'informations, reportez-vous à la section Gestion des listes sécurisées et dangereuses pour CylancePROTECT Desktop.

4. Modifiez la stratégie de terminal pour activer les analyses de détection des menaces en arrière-plan afin d'analyser les fichiers exécutables qui peuvent être des menaces inactives sur le disque.
   a) Dans l'onglet **Paramètres de protection**, activez le paramètre **Détection des menaces en arrière-plan** et sélectionnez l'option **Exécuter une fois**. Bien que l'analyse périodique ne soit pas nécessaire en raison des capacités prédictives de la solution, vous pouvez sélectionner **Exécution récurrente** pour l'activer, par exemple, à des fins de conformité.
   b) Activez le paramètre **Contrôler les nouveaux fichiers**. Ce paramètre peut avoir un impact négatif sur les performances du terminal. L'ajout d'exclusions de dossiers peut contribuer à réduire l'impact.
   c) Pour exclure des dossiers spécifiques de la détection des menaces en arrière-plan, sélectionnez **Exclure des dossiers spécifiques (y compris les sous-dossiers)** et spécifiez les dossiers à exclure. Pour autoriser l'exécution des fichiers dans les dossiers que vous avez spécifiés, sélectionnez **Autoriser l'exécution**. Pour en savoir plus sur ces champs, reportez-vous à Paramètres de protection.
   d) Cliquez sur **Enregistrer** pour enregistrer la stratégie.
   e) Testez à nouveau la stratégie et assurez-vous que toutes les applications que les utilisateurs doivent utiliser sont autorisées à s'exécuter. L'analyse de détection des menaces en arrière-plan peut prendre jusqu'à une semaine, en fonction de l'activité du système et du nombre de fichiers qui doivent être analysés. Si nécessaire, assurez-vous d'ajouter des fichiers à la liste sécurisée des stratégies, à la liste sécurisée globale ou de les supprimer pour des terminaux individuels. Vous pouvez également exclure le dossier contenant le fichier dans les paramètres de protection.
5. Modifiez la stratégie de terminal pour éliminer les processus dangereux en cours d'exécution sur le système. Par exemple, lorsqu'une menace est détectée dans un fichier exécutable (.exe ou .msi) et qu'elle est considérée comme dangereuse, ce paramètre interrompt les processus en cours d'exécution et leurs sous-processus.
   a) Dans l'onglet **Paramètres de protection**, activez le paramètre **Arrêter les processus en cours d'exécution dangereux**.
6. Modifiez la stratégie afin d'activer les paramètres de mise en quarantaine automatique pour les fichiers dangereux et anormaux.
   a) Dans l'onglet **Actions de fichier**, sous la colonne de tableau **Dangereux**, activez le paramètre **Mise en quarantaine automatique** en regard de l'**Exécutable** pour déplacer automatiquement les fichiers dangereux vers le dossier de quarantaine du terminal. Les fichiers dangereux ont des attributs de programmes malveillants et sont susceptibles d'être des programmes malveillants.
   b) Sous **Anormal**, activez **Quarantaine automatique** pour déplacer automatiquement les fichiers anormaux vers le dossier de quarantaine du terminal. Un fichier anormal possède moins d'attributs de programme malveillant qu'un fichier dangereux et est moins susceptible d'être un programme malveillant.
7. Modifiez la stratégie pour activer les paramètres de protection de la mémoire afin de gérer les failles de mémoire, les injections de processus et les escalades.
   a) Dans l'onglet **Actions de mémoire** de la stratégie de terminal, activez **Protection de la mémoire** et définissez les types de violation sur **Alerter**. Lorsqu'un type de violation est défini sur Alerte et qu'une menace de ce type est détectée, l'agent envoie des informations à la console, mais ne bloque ni ne met fin aux processus en cours d'exécution dans la mémoire du terminal.
   b) Lors du test de la stratégie, accédez à **Protection > Protection de la mémoire** de la console afin d'afficher la liste des alertes de protection de la mémoire pour les processus pouvant constituer une menace.
   c) Si vous avez déterminé que l'un des processus est sûr pour les activités quotidiennes de l'entreprise, vous pouvez ajouter des exclusions pour les processus que vous souhaitez autoriser à exécuter. Dans l'onglet **Actions de mémoire** de la stratégie de terminal, cliquez sur **Ajouter une exclusion** et spécifiez le chemin relatif vers le fichier.
   d) Une fois que vous avez spécifié les exclusions pour les processus que vous souhaitez autoriser à exécuter, définissez l'action sur **Bloquer** pour tous les types de violation. Lorsqu'un type de violation est bloqué, l'agent envoie des informations à la console et empêche le processus malveillant de s'exécuter dans la mémoire. L'application qui a appelé le processus malveillant est autorisée à poursuivre son exécution.

8. Modifiez la stratégie pour activer les paramètres de contrôle du terminal. Cet exemple montre comment bloquer l'accès à tous les types de terminaux et autoriser les exceptions. Cependant, vous pouvez choisir d'autoriser l'accès complet à tous les types de terminaux et de bloquer les exceptions à la place.
   a) Dans l'onglet **Contrôle du terminal** de la stratégie de terminal, activez la stratégie **Contrôle du terminal**.
   b) Définissez le niveau d'accès de chaque type de périphérique USB sur **Accès complet**.
   c) Enregistrez la stratégie.
   d) Sur le terminal test, insérez un périphérique USB.
   e) Dans la console de gestion, accédez à **Protection > Terminaux externes** et identifiez l'ID fournisseur, l'ID produit et le numéro de série des terminaux que vous souhaitez autoriser. Tous les fabricants n'utilisent pas un numéro de série unique avec leurs produits ; certains fabricants utilisent le même numéro de série pour plusieurs produits.
   f) Dans l'onglet **Contrôle de terminal** de la stratégie de terminal, dans la section **Liste d'exclusion du stockage externe**, cliquez sur **Ajouter un terminal** pour ajouter les terminaux que vous souhaitez autoriser.
   g) Une fois le test terminé, définissez le niveau d'accès de chaque type de terminal sur **Bloquer**. Vous pouvez ajouter des exclusions si nécessaire.
9. Modifiez la stratégie pour activer les paramètres de contrôle du script. Le temps de test suggéré est de 1 à 3 semaines.
   a) Dans l'onglet **Contrôle de script** de la stratégie de terminal, activez la stratégie **Contrôle de script**.
   b) Définissez la stratégie pour chacun des types de script sur **Alerter**. Plus la durée d'alerte du contrôle des scripts est longue, plus vous êtes susceptible de trouver des scripts rarement utilisés dans l'organisation.

      **Remarque :** L'activation du paramètre de contrôle de script peut entrainer un volume élevé d'évènements si des scripts sont utilisés pour gérer les paramètres Active Directory.
   c) Accédez à **Protection > Contrôle de script** et identifiez les scripts qui ont été exécutés sur les terminaux que vous souhaitez autoriser.
   d) Dans l'onglet **Contrôle de script** de la stratégie de terminal, dans la section **Exclure des fichiers, scripts ou processus**, cliquez sur **Ajouter une exclusion** et spécifiez un chemin de processus relatif pour les scripts que vous souhaitez autoriser (par exemple, `\Cases\AllowedScripts`).
   e) Une fois que vous avez ajouté les exclusions pour les scripts que vous souhaitez autoriser à exécuter, vous pouvez définir la stratégie pour chacun des types de script sur **Bloquer**.

## Exclusions et quand les utiliser

Le tableau suivant fournit une description de chaque type d'exclusion et des conseils généraux sur la manière et le moment de les utiliser de manière appropriée.

| Type d'exclusion | Description et exemple |
| --- | --- |
| Liste sécurisée des stratégies (actions de fichier) | La liste de sécurité de la stratégie est spécifiée dans l'onglet **Actions de fichier** d'une stratégie de terminal.<br><br>Lorsqu'une stratégie de terminal est attribuée à un terminal, celui-ci est autorisé à exécuter les fichiers spécifiés dans la liste de sécurité des stratégies. La liste de sécurité de la stratégie est appliquée au niveau de la stratégie pour des terminaux spécifiques, tandis que la liste de sécurité globale ou la liste de quarantaine est appliquée au niveau global pour tous les terminaux. La liste sécurisée des stratégies est prioritaire sur la liste de quarantaine globale. Un fichier ajouté à la liste de sécurité des règles peut s'exécuter sur n'importe quel terminal auquel la règle est attribuée, même si ce fichier figure dans la liste de quarantaine globale, ce qui empêche l'exécution des fichiers sur tous les terminaux.<br><br>Exemple : si vous utilisez fréquemment des outils d'escalade des privilèges tels que PSEXEC pour effectuer vos tâches quotidiennes. Vous ne voulez pas que les autres utilisateurs aient la même capacité et vous voulez les empêcher d'utiliser ces outils sans affecter vos tâches quotidiennes. Pour ce faire, vous pouvez ajouter PSEXEC à la liste de quarantaine globale et ajouter le même hachage de fichier à votre liste sécurisée des stratégies. Vous devez ensuite vous assurer que seuls vous et les autres utilisateurs autorisés êtes affectés à la stratégie de terminal spécifique dans laquelle vous avez ajouté PSEXEC à la liste sécurisée. Ainsi, PSEXEC sera mis en quarantaine pour tous les utilisateurs qui ne sont pas affectés à la stratégie de terminal, mais les utilisateurs affectés à la stratégie de terminal pourront l'utiliser. |

| Type d'exclusion | Description et exemple |
| --- | --- |
| Exclure les fichiers exécutables ou les macros (protection de la mémoire) | Les exclusions de la stratégie de protection de la mémoire sont spécifiées dans l'onglet **Actions de mémoire** d'une stratégie de terminal lorsque la **Protection de la mémoire** est activée.<br><br>Lorsque vous spécifiez des exclusions pour la protection de la mémoire, l'agent ignore les violations de types spécifiques de chaque application spécifique. En d'autres termes, vous évitez de bloquer ou de fermer une application lorsqu'elle exécute une action qui entraine une violation d'un certain type.<br><br>Lorsque la protection de la mémoire est activée, l'agent surveille les processus d'application pour détecter les actions spécifiques qu'il effectue. Si un processus exécute une action particulière que l'agent surveille, telle qu'une lecture LSASS, l'agent réagit à cette action en fonction de la stratégie de terminal. Il arrive parfois que des faux positifs se produisent et que la protection de la mémoire bloque une action qu'une application a tenté d'exécuter ou arrête complètement l'application. Dans ce cas, vous pouvez spécifier des exclusions pour la protection de la mémoire afin que certaines applications soient exemptes de types de violation spécifiques et puissent s'exécuter comme prévu sans être bloquées ou interrompues.<br><br>Exemple : par défaut, votre organisation bloque toutes les violations de protection de la mémoire de toutes les applications. Vous utilisez fréquemment Test.exe et vous comprenez qu'il a des raisons légitimes de violations de lecture LSASS uniquement. Vous pouvez ajouter une exclusion afin que l'agent ignore uniquement les violations de lecture LSASS du fichier Test.exe. L'agent bloque toujours Test.exe lorsqu'une violation de tout autre type se produit.<br><br>Les exclusions de protection de la mémoire utilisent des chemins relatifs (les lettres de lecteur ne sont pas requises) et peuvent être spécifiées jusqu'au niveau exécutable. Par exemple :<br><br>• `\Application\Subfolder\Test.exe`<br>• `\Subfolder\executable`<br><br>**Remarque :** Il n'est pas recommandé de spécifier une exclusion au niveau de l'exécutable sans chemin relatif. Par exemple, si une exclusion est définie pour `\Test.exe`, un fichier malveillant portant le même nom est autorisé à s'exécuter à partir de n'importe quel dossier du terminal. |

| Type d'exclusion | Description et exemple |
| --- | --- |
| Exclure des dossiers spécifiques (Paramètres de protection) | Les exclusions pour la détection des menaces en arrière-plan sont spécifiées dans l'onglet **Paramètres de protection** d'une stratégie de terminal lorsque la **Détection des menaces en arrière-plan** est activée. Cette exclusion peut également être appelée « liste sécurisée de répertoires ». Lorsqu'un répertoire est exclu, l'agent ignore tous les fichiers de ce répertoire lors d'une analyse, y compris les sous-dossiers.<br><br>Si vous sélectionnez **Autoriser l'exécution**, l'agent ignore tous les exécutables lancés à partir des répertoires exclus.<br><br>Exemple : un développeur d'applications de votre organisation utilise un répertoire (par exemple, `C:\DevFiles\Temp`) pour stocker les fichiers temporaires générés lors de la compilation. L'agent analyse ces fichiers, les considère comme dangereux en raison des différentes caractéristiques qu'ils contiennent, puis les met en quarantaine. Le développeur soumet une demande pour autoriser le répertoire temporaire. Vous pouvez ajouter le répertoire `C:\DevFiles\Temp` afin que les fichiers temporaires soient ignorés et que le développeur puisse effectuer son travail. |
| Exclusions de dossiers (Contrôle de script) | Les exclusions de la stratégie de contrôle des scripts sont spécifiées dans l'onglet **Contrôle de script** d'une stratégie de terminal lorsque le **contrôle de script** est activé. Vous pouvez ajouter des exclusions lorsque vous souhaitez autoriser l'exécution de scripts dans un répertoire spécifié. Lors de l'ajout d'exclusions de contrôle de script, spécifiez les chemins relatifs. Les sous-dossiers sont également inclus dans l'exclusion.<br><br>Exemple : un administrateur informatique tente d'exécuter un script situé dans `C:\Scripts\Subfolder\Test`. Le script est bloqué par le contrôle de script chaque fois que l'administrateur informatique tente d'exécuter le script. Pour permettre l'exécution du script, vous pouvez ajouter l'un des chemins relatifs suivants en tant qu'exclusion de la stratégie de contrôle du script :<br><br>• `\Scripts\Subfolder\Test`<br>• `\Subfolder\Test\`<br>• `\Scripts\Subfolder\`<br>• `\Scripts\`<br>• `\Subfolder\`<br>• `\Test\` |

# Utiliser les stratégies de terminal pour gérer les terminaux CylancePROTECT Desktop

Les stratégies de terminal définissent la manière dont l'agent CylancePROTECT Desktop gère les fichiers suspects et les logiciels malveillants qu'il rencontre. Le contrôle de l'exécution est activé par défaut dans toutes les stratégies de terminal, ce qui permet à l'agent d'alerter la console de gestion lorsque des fichiers dangereux ou anormaux tentent de s'exécuter. Une fois l'agent installé, il analyse également tous les processus et modules

en cours d'exécution pour déterminer s'il existe des menaces déjà actives. Chaque terminal est attribué à une stratégie de terminal. La stratégie par défaut est attribuée si aucune autre stratégie n'est attribuée à un terminal.

Vous pouvez utiliser les stratégies de terminal pour faire ce qui suit :

- Activez la mise en quarantaine automatique pour les fichiers non sécurisés ou anormaux afin qu'ils ne puissent pas s'exécuter sur le terminal. Vous pouvez définir la liste de sécurité des règles pour les fichiers que votre entreprise considère comme surs, même si les fichiers ont un indice de menace qui indique qu'ils sont dangereux ou anormaux.
- Activez les paramètres de protection de la mémoire pour empêcher les failles de mémoire, y compris les injections de processus et les escalades. Vous pouvez ajouter des exclusions pour les fichiers exécutables et macros que vous souhaitez autoriser à exécuter.
- Activez les paramètres de protection tels que la prévention de l'arrêt du service CylancePROTECT, la suppression des processus et sous-processus dangereux en cours d'exécution et l'exécution de la détection des menaces en arrière-plan pour analyser les fichiers qui peuvent être des menaces en sommeil.
- Activez et configurer les paramètres de CylanceOPTICS.
- Activez la fonction de contrôle des applications pour empêcher l'exécution de nouvelles applications et bloquer toute mise à jour ou modification des applications déjà installées.
- Activez les paramètres de l'agent, tels que le téléchargement automatique de fichiers journaux ou les notifications de bureau.
- Activez les paramètres de contrôle des scripts pour empêcher l'exécution de scripts malveillants sur les terminaux. Vous pouvez ajouter des exclusions pour permettre l'exécution de certains scripts si votre organisation les considère comme sures.
- Activez les paramètres de contrôle des terminaux pour empêcher les terminaux de stockage de masse USB (tels que les clés USB, les disques durs externes et les smartphones) de se connecter à un terminal.

## Créer et gérer une stratégie de terminal

Les stratégies de terminal vous permettent de contrôler les fonctionnalités des agents CylancePROTECT Desktop et CylanceOPTICS. Vous pouvez créer différentes stratégies de terminal pour répondre aux différents besoins des groupes au sein d'une organisation.

1. Sur la barre de menus de la console de gestion, cliquez sur **Stratégies > Stratégie de terminal**.
2. Effectuez l'une des opérations suivantes :

| Tâche | Étapes |
|---|---|
| Ajouter une nouvelle stratégie de terminal | **a.** Cliquez sur **Ajouter une nouvelle stratégie**.<br>**b.** Dans le champ **Nom de la stratégie**, saisissez le nom de la stratégie de terminal.<br>**c.** Sélectionner les paramètres de la stratégie de terminal<br>**d.** Cliquez sur **Créer**. |
| Modifier une stratégie de terminal | **a.** Cliquez sur le nom de la stratégie de terminal que vous souhaitez modifier.<br>**b.** Mettez à jour les paramètres de la stratégie de terminal.<br>**c.** Cliquez sur **Enregistrer**. |

| Tâche | Étapes |
| --- | --- |
| Copier une stratégie de terminal | **a.** Cliquez sur le nom de la stratégie informatique que vous souhaitez copier.<br>**b.** Dans le champ **Nom de la stratégie**, modifiez le nom de la stratégie de terminal.<br>**c.** Si nécessaire, mettez à jour les paramètres de la stratégie de terminal.<br>**d.** Cliquez sur **Enregistrer sous**. |
| Paramètres de la stratégie de terminal | Pour plus d'informations sur les paramètres de stratégie de terminal, reportez-vous aux sections suivantes :<br>• Actions de fichier<br>• Actions de mémoire<br>• Paramètres de protection<br>• Contrôle d'applications<br>• Paramètres de l'agent<br>• Contrôle de script<br>• Contrôle du terminal<br>• Paramètres CylanceOPTICS |
| Attribuer automatiquement une stratégie de terminal aux terminaux d'une zone | Vous pouvez spécifier une stratégie de terminal lorsque vous configurez une zone de sorte que lorsque des terminaux sont ajoutés à cette zone, ils sont automatiquement attribués à une stratégie. Pour plus d'informations, reportez-vous à Ajouter et configurer une zone. |
| Attribuer manuellement une stratégie de terminal à un terminal | **a.** Dans la barre de menus de la console de gestion , cliquez sur **Actifs > Terminaux**.<br>**b.** Sélectionnez les terminaux auxquels vous souhaitez attribuer une stratégie de terminal.<br>**c.** Cliquez sur **Attribuer la stratégie**.<br>**d.** Sélectionnez la stratégie de terminal que vous souhaitez attribuer.<br>**e.** Cliquez sur **Enregistrer**. |

## Actions de fichier

Les paramètres suivants se trouvent dans l'onglet **Actions sur les fichiers** d'une stratégie de terminal. Ils spécifient comment l'agent CylancePROTECT Desktop gère un fichier lorsqu'il détecte une menace qu'il considère comme dangereuse ou anormale.

| Option | Description |
| --- | --- |
| **Mise en quarantaine automatique avec contrôle d'exécution** | Ce paramètre spécifie s'il faut mettre automatiquement en quarantaine les fichiers non sécurisés ou anormaux pour les empêcher de s'exécuter. Si vous souhaitez mettre en quarantaine des fichiers anormaux, vous devez d'abord sélectionner l'option de mise en quarantaine des fichiers non sécurisés. Les fichiers dangereux contiennent beaucoup plus d'attributs de logiciels malveillants et sont plus susceptibles d'être des logiciels malveillants que les fichiers anormaux.<br><br>Lorsqu'un fichier est mis en quarantaine, les évènements suivants se produisent :<br>• Le fichier est renommé avec l'extension `.quarantine`.<br>• Le fichier est déplacé de son emplacement d'origine vers l'un des répertoires de quarantaine suivants :<br>  • **Pour les terminaux Windows :** `C:\ProgramData\Cylance\Desktop\q`<br>  • **Pour les terminaux macOS :** `/Library/Application Support/Cylance/Desktop/q`<br>  • **Pour les terminaux Linux :** `/opt/cylance/desktop/q`<br>• La liste de contrôle d'accès (ACL) pour le fichier est modifiée pour empêcher l'utilisateur d'interagir avec le fichier.<br><br>Certains logiciels malveillants sont conçus pour créer des fichiers dans d'autres répertoires et continuent de le faire jusqu'à ce qu'il réussisse. Au lieu de supprimer les fichiers, CylancePROTECT Desktop les modifie afin que le logiciel malveillant n'essaie pas de les créer à nouveau et qu'ils ne puissent pas être exécutés. |
| **Activer la suppression automatique des fichiers mis en quarantaine** | Ce paramètre spécifie s'il faut supprimer automatiquement les fichiers mis en quarantaine après un nombre de jours spécifié. Par exemple, vous pouvez le définir de sorte qu'un fichier soit supprimé après qu'il a été mis en quarantaine pendant 14 jours. Le nombre de jours peut être compris entre 14 et 365.<br><br>Lorsque le fichier est supprimé, les évènements suivants se produisent :<br>• L'action est incluse dans le fichier journal de l'agent à des fins de vérification et d'audit.<br>• Le fichier est supprimé de la liste de quarantaine dans l'interface utilisateur de l'agent. |
| **Chargement automatique** | Assurez-vous d'activer **Chargement automatique** pour tous les types de fichiers disponibles. Si l'agent trouve un fichier que les services cloud CylancePROTECT n'ont jamais analysé auparavant, ils lui demandent de télécharger le fichier pour analyse.<br><br>CylancePROTECT Desktop charge et analyse uniquement les fichiers inconnus tels que les fichiers Portable Executable (PE), Executable and Linkable Format (ELF) et Mach Object File format (Mach-O). Si le même fichier inconnu est découvert sur plusieurs terminal de l'organisation, CylancePROTECT Desktop télécharge un seul fichier à partir d'un seul terminal pour analyse, et non un fichier par terminal. |
| **Liste sécurisée de stratégies** | Ajoutez les fichiers que vous considérez comme surs à la liste de sécurité des règles pour les autoriser à s'exécuter. La liste de sécurité de la stratégie a la priorité sur la liste sécurisée globale ou la liste de quarantaine globale. Par exemple, un fichier ajouté à la liste de sécurité des règles peut s'exécuter sur n'importe quel terminal auquel la règle est attribuée, même si ce fichier figure dans la liste de quarantaine globale, ce qui empêche l'exécution des fichiers sur tous les terminaux. |

#### Ajouter des fichiers à la liste sécurisée des stratégies

Vous pouvez ajouter des fichiers à la liste de sécurité de la stratégie afin que tous les agents de cette stratégie les considèrent comme surs, même si l'indice de menace indique qu'ils sont dangereux ou anormaux. Pour en savoir plus sur la liste sécurisée de stratégies, consultez Exclusions et quand les utiliser.

**Avant de commencer :** Obtenez la valeur SHA256 du fichier que vous souhaitez exclure de l'écran **Protection > Menaces**.

1. Sur la barre de menus de la console de gestion, cliquez sur **Stratégies > Stratégie de terminal**.
2. Cliquez sur le nom d'une stratégie pour la modifier ou cliquez sur **Ajouter une nouvelle stratégie**.
3. Dans l'onglet **Actions sur les fichiers**, dans la section **Liste sécurisée de stratégies**, cliquez sur **Ajouter un fichier**.
4. Spécifiez la valeur SHA256 pour le fichier que vous souhaitez exclure.
5. Vous pouvez également spécifier la valeur MD5 et le nom du fichier.
6. Sélectionnez une catégorie et saisissez le motif de cette exclusion.
7. Cliquez sur **Envoyer**.

### Actions de mémoire

Les paramètres suivants se trouvent dans l'onglet **Actions de mémoire** d'une stratégie de terminal. Vous pouvez activer **Protection de la mémoire** et spécifier la manière dont l'agent CylancePROTECT Desktop gère les failles de mémoire, y compris les injections de processus et les escalades. Vous pouvez également ajouter des fichiers exécutables à une liste d'exclusion, ce qui permet à ces fichiers de s'exécuter lorsque cette règle est appliquée.

| Option | Description |
|---|---|
| **Protection de la mémoire** | Ce paramètre indique s'il faut activer les paramètres de protection de la mémoire dans cette stratégie. Lorsque cette option est activée, l'agent détecte différents types d'appels de processus qui peuvent constituer une menace et gère chaque type en fonction du paramètre que vous choisissez.<br>• **Ignorer** : l'agent n'effectue aucune action.<br>• **Alerter** : l'agent consigne la violation et signale l'incident à la console de gestion.<br>• **Bloquer** : l'agent consigne la violation, signale l'incident à la console de gestion et bloque l'appel de traitement. L'application qui a passé l'appel est autorisée à continuer à s'exécuter.<br>• **Terminer** : l'agent consigne la violation, signale l'incident à la console de gestion, bloque l'appel de traitement et met fin à l'application qui a effectué l'appel. |

| Option | Description |
| --- | --- |
| **Exclure les fichiers exécutables** | Ce paramètre spécifie le chemin relatif des fichiers que vous souhaitez ignorer. Lorsque des fichiers sont ajoutés à cette liste d'exclusion, vous les autorisez à s'exécuter ou à être installés sur les terminaux auxquels cette règle est attribuée.<br><br>Vous spécifiez le chemin relatif du fichier et les types de violation que vous souhaitez ignorer. Sous Windows, vous pouvez également spécifier le chemin d'accès absolu au fichier. Utilisez des chemins relatifs raccourcis avec précaution, car il peut exclure d'autres exécutables qui ont le même chemin relatif.<br><br>Après avoir appliqué l'exclusion, toutes les instances de ce processus doivent être terminées pour empêcher le pilote de s'y injecter.<br><br>**Exemples sous Windows**<br><br>• Chemin relatif : `\Application\Subfolder\application.exe`<br>• Chemin absolu : `C:\Application\Subfolder\application.exe`<br><br>**Exemples sous Linux**<br><br>• Chemin relatif : `/opt/application/executable`<br>• Chemin relatif des fichiers de bibliothèque dynamique : `/executable.dylib`<br><br>**Exemples sous macOS**<br><br>• Chemin relatif sans espaces : `/Applications/SampleApplication.app/Contents/MacOS/executable`<br>• Chemin relatif avec espaces : `/Applications/Sample Application.app/Contents/MacOS/executable`<br>• Chemin relatif des fichiers de bibliothèque dynamique : `/executable.dylib`<br><br>Vous pouvez également utiliser des caractères génériques pour les exclusions de protection de la mémoire. Pour plus d'informations, reportez-vous à Caractères génériques dans les exclusions de protection de la mémoire.<br><br>**Remarque :** Si vous enregistrez une exclusion sans ajouter au moins un type de violation à ignorer, l'exclusion est appliquée aux événements de protection de la mémoire et de contrôle de script. L'ajout d'au moins un type de violation à ignorer signifie que l'exclusion est appliquée à la protection de la mémoire uniquement. |

| Option | Description |
| --- | --- |
| **Ignorer des types de violation spécifiques** | Lorsque vous ajoutez une exclusion, cochez cette case pour ignorer une violation de fichier basée sur un ou l'ensemble des éléments suivants :<br>• Types de catégories de violation (par exemple, Exploitation, Injection de processus, Escalade)<br>• Types de violations individuelles sous chaque catégorie (par exemple, Pivot de pile, Allocation à distance de mémoire, Attribution nulle, etc.)<br>Lorsque vous ajoutez des exclusions à une stratégie de protection de la mémoire, si vous souhaitez que la stratégie s'applique uniquement aux violations de protection de la mémoire et non aux violations de contrôle de script, spécifiez au moins un type de violation que vous souhaitez ignorer. Si vous ne sélectionnez aucun type de violation à ignorer, un message d'avertissement s'affiche et l'exclusion s'applique à la fois aux stratégies de protection de la mémoire et de contrôle des scripts.<br>Pour les stratégies de protection de la mémoire existantes :<br>• Si le paramètre d'exclusion **Ignorer des types de violation spécifiques** est déjà coché mais que la stratégie de contrôle des scripts n'est pas activée, aucune action n'est requise.<br>• Si le paramètre d'exclusion **Ignorer des types de violation spécifiques** n'est pas coché et que vous souhaitez vous assurer que la stratégie est appliquée uniquement aux violations de protection de la mémoire (et non au contrôle de script), vous devez le cocher et spécifier au moins un type de violation que vous souhaitez ignorer.<br>Si vous modifiez une stratégie existante et que vous ajoutez une exclusion, la case à cocher Ignorer les types de violation spécifiques ne s'affiche pas tant que vous n'avez pas modifié le type de violation (par exemple, déplacez-la de Bloquer à Terminer ou Alerte).<br>Pour chaque fichier dont les types de violation spécifiques sont ignorés, vous pouvez afficher des informations détaillées, modifier ou supprimer les paramètres. |
| **Exclusion Traiter en tant que DLL** | Sélectionnez ce paramètre lorsque vous souhaitez ajouter des exclusions pour les DLL tierces. Par exemple, si vous exécutez des produits de sécurité tiers outre CylancePROTECT Desktop pour Windows, vous pouvez ajouter une exclusion aux fichiers .dll appropriés afin que CylancePROTECT ignore les violations spécifiques de ces produits. Cette fonctionnalité prend uniquement en charge les types de violation Charge utile malveillante et Écrasement de la DLL système.<br>Les règles suivantes s'appliquent lorsque vous spécifiez une exclusion de la DLL :<br>• Vous devez sélectionner l'option **Exclusion Traiter en tant que DLL** dans la stratégie de terminal.<br>• Le terminal doit exécuter l'agent CylancePROTECT Desktop 3.1.1001 ou une version ultérieure sur un terminal Windows.<br>• Le chemin d'accès au fichier que vous spécifiez doit correspondre au chemin complet et direct vers le fichier .dll. Les caractères génériques ne sont pas autorisés.<br>• Le fichier .dll doit être signé à l'aide d'un certificat approuvé sur le terminal sur lequel CylancePROTECT Desktop est installé. Dans le cas contraire, il ne sera pas exclu.<br>Pour en savoir plus sur la prise en charge des exclusions de DLL, rendez-vous sur support.blackberry.com pour consulter l'article 108909 de la base de connaissances. |

**Types de violations de protection de la mémoire**

**Types de violation par exploitation**

| Type de violation | Description | Système d'exploitation pris en charge |
|---|---|---|
| **Pivot de pile** | La pile d'un thread a été remplacée par une pile différente. En général, le système alloue une seule pile pour un thread. Un utilisateur malveillant pourrait utiliser une pile différente pour contrôler l'exécution en évitant le blocage de la stratégie de prévention de l'exécution des données. | Windows<br>macOS*<br>Linux |
| **Protection de pile** | La protection de la mémoire d'une pile de thread a été modifiée pour activer l'autorisation d'exécution. La mémoire de la pile ne doit pas être exécutable ; en général, cela peut signifier qu'un utilisateur malveillant prépare l'exécution de code malveillant stocké dans la mémoire de la pile en vue d'une exploitation, tentative qui serait normalement bloquée par la prévention de l'exécution des données. | Windows<br>macOS*<br>Linux |
| **Écraser le code** | Le code résidant dans la mémoire d'un processus a été modifié à l'aide d'une technique qui peut indiquer une tentative de contournement de la stratégie de prévention de l'exécution des données. | Windows |
| **Extraction de RAM** | Un processus tente de lire des données de piste à bande magnétique valides à partir d'un autre processus. En général, cette violation est associée aux systèmes de point de vente (POS). | Windows |
| **Charge utile malveillante** | Un shellcode et une charge utile génériques associés à l'exploitation ont été détectés.<br>Ce type de violation de protection de la mémoire prend en charge les exclusions DLL. | Windows |
| **Types de violations disponibles avec l'agent 2.1.1580 ou une version ultérieure** | | |
| **Surveillance des appels système** | Un appel système effectué vers une application ou un système d'exploitation a été détecté. | Windows |
| **Appels système directs** | Une tentative d'injection silencieuse de code malveillant dans d'autres processus a été détectée. Ce type de violation ne peut pas être bloqué. | Windows |
| **Écrasement de la DLL système** | Une tentative d'écrasement d'une DLL système a été détectée.<br>Ce type de violation de protection de la mémoire prend en charge les exclusions DLL. | Windows |

| Type de violation | Description | Système d'exploitation pris en charge |
|---|---|---|
| **Objet COM dangereux** | Un code malveillant référençant un objet COM (Component Object Model) a été détecté. | Windows |
| **Injection via APC** | Un processus injectant un code arbitraire dans le processus cible en utilisant un appel de procédure asynchrone (APC) ou un thread distant de démarrage pour appeler `LoadLibrary`, ou une fonction similaire, a été détecté.<br><br>Si cette stratégie est définie sur Alerte, vous pouvez vous attendre à voir des alertes pour les injections valides et malveillantes se produisant pour les applications sur les terminaux Windows. L'alerte signale l'application qui a reçu l'injection, mais vous devez déterminer la source exécutable à l'origine de l'alerte. Pour plus d'informations sur la collecte des données nécessaires qui peuvent vous aider à déterminer si une injection était valide ou malveillante, consultez l'article 92422 de la base de connaissances sur support.blackberry.com.<br><br>Si cette règle est définie sur Bloquer ou Terminer, elle empêche l'exécution des applications signalées sur le terminal, même si elles sont valides. Cela peut perturber les activités quotidiennes d'un utilisateur. | Windows |
| **Types de violation disponibles avec l'agent 3.0.1000 ou version ultérieure** | | |
| **Macros VBA dangereuses** | Une macro contenant des implémentations dangereuses a été détectée.<br><br>Ce paramètre protège les terminaux exécutant l'agent version 2.1.1580 et versions ultérieures contre les macros malveillantes. Les exclusions spécifiées dans la stratégie de protection de la mémoire sont prises en charge par l'agent version 3.0 et versions ultérieures.<br><br>Pour protéger les terminaux exécutant l'agent version 2.1.1578 et ses versions antérieures contre les macros malveillantes, activez et configurez la stratégie de contrôle des scripts et ses exclusions. | Windows |

* Pris en charge uniquement sur macOS Catalina et les versions antérieures.

**Types de violation par injection de processus**

| Type de violation | Description | Système d'exploitation pris en charge |
|---|---|---|
| **Allocation à distance de mémoire** | Un processus a alloué de la mémoire dans un autre processus. La plupart des allocations se produisent uniquement dans un seul processus. Cela peut indiquer une tentative d'injection de code ou de données dans un autre processus, pour renforcer une présence malveillante sur un système. | Windows<br>macOS |
| **Mappage à distance de la mémoire** | Un processus a introduit du code ou des données dans un autre processus. Cela peut indiquer une tentative de démarrage de l'exécution du code dans un autre processus pour renforcer une présence malveillante. | macOS |
| **Écriture à distance dans la mémoire** | Un processus a modifié la mémoire dans un autre processus. Il peut s'agir d'une tentative de stockage de code ou de données dans la mémoire précédemment allouée (voir `OutOfProcessAllocation`), mais il est possible qu'un utilisateur malveillant tente d'écraser la mémoire existante pour détourner l'exécution à des fins malveillantes. | Windows<br>macOS |
| **Écriture à distance de PE dans la mémoire** | Un processus a modifié la mémoire dans un autre processus pour contenir une image exécutable. En général, cela indique qu'un utilisateur malveillant tente d'exécuter du code sans l'écrire sur le disque au préalable. | Windows |
| **Écrasement du code à distance** | Un processus a modifié la mémoire exécutable dans un autre processus. Dans des conditions normales, la mémoire exécutable n'est pas modifiée, notamment par un autre processus. Cela indique généralement une tentative de déviation d'une exécution vers un autre processus. | Windows |
| **Annulation du mappage à distance de la mémoire** | Un processus a supprimé un exécutable Windows de la mémoire d'un autre processus. Cela peut indiquer une tentative de remplacement de l'image exécutable par une copie modifiée afin d'en détourner l'exécution. | Windows<br>macOS |
| **Création de thread à distance** | Un processus a créé un nouveau thread dans un autre processus. En général, les threads sont uniquement créés par un même processus. Un utilisateur malveillant utilise généralement cette méthode pour activer une présence malveillante qui a été injectée dans un autre processus. | Windows<br>macOS* |
| **Planification APC à distance** | Un processus a dévié l'exécution du thread d'un autre processus. Généralement, un utilisateur malveillant utilise généralement cette méthode pour activer une présence malveillante qui a été injectée dans un autre processus. | Windows |

| Type de violation | Description | Système d'exploitation pris en charge |
|---|---|---|
| **Injection de DYLD** | Une variable d'environnement a été définie pour entrainer l'injection d'une bibliothèque partagée dans un processus lancé. Les attaques peuvent modifier la liste d'applications telles que Safari, ou remplacer des applications par des scripts bash, ce qui autorise le chargement automatique de leurs modules lors du démarrage d'une application. | macOS*<br>Linux |
| **Types de violations disponibles avec l'agent 2.1.1580 ou une version ultérieure** | | |
| **Typosquattage** | Un nouveau processus malveillant a été lancé à partir d'un fichier non encore écrit dans le système de fichiers. La transaction d'écriture de fichier est généralement annulée après le démarrage du processus (de sorte que le fichier malveillant ne soit jamais validé sur le disque) et toute tentative d'analyse du fichier sur le disque obtiendra uniquement un fichier inoffensif non modifié. | Windows |
| **Variable d'environnement dangereuse** | Une variable d'environnement potentiellement associée à un programme malveillant a été détectée. | Windows |

* Pris en charge uniquement sur macOS Catalina et les versions antérieures.

#### Types de violation par escalade

| Type de violation | Description | Système d'exploitation pris en charge |
|---|---|---|
| **Lecture LSASS** | La mémoire appartenant au processus d'autorité de sécurité locale de Windows a fait l'objet d'un accès indiquant une tentative d'obtention des mots de passe des utilisateurs. | Windows |
| **Attribution nulle** | Une page nulle a été affectée. La zone de mémoire est généralement réservée, mais dans certaines circonstances, elle peut être allouée. Les attaques peuvent l'utiliser pour configurer l'escalade des privilèges en profitant d'un exploit de référence nulle connu, généralement dans le noyau. | Windows<br>macOS* |
| **Types de violations disponibles avec l'agent 2.1.1580 ou une version ultérieure** | | |
| **Modifications des autorisations de mémoire dans d'autres processus** | Un processus en violation a modifié les autorisations d'accès à la mémoire dans un autre processus. L'objectif est généralement d'injecter du code dans un autre processus et de rendre la mémoire exécutable en modifiant ses autorisations d'accès. | Windows |

| Type de violation | Description | Système d'exploitation pris en charge |
|---|---|---|
| **Modifications des autorisations de mémoire dans des processus enfants** | Un processus en violation a créé un processus enfant et a modifié les autorisations d'accès à la mémoire dans celui-ci. | Windows |
| **Jeton système volé** | Un jeton d'accès a été modifié pour permettre à un utilisateur de contourner les contrôles d'accès de sécurité. | Windows |
| **Début du processus à faible intégrité** | Un processus a été configuré pour s'exécuter avec un niveau d'intégrité faible. | Windows |

* Pris en charge uniquement sur macOS Catalina et les versions antérieures.

#### Caractères génériques dans les exclusions de protection de la mémoire

Les exclusions de protection de la mémoire peuvent inclure les caractères spéciaux suivants (tous les systèmes d'exploitation) : ^ & ' @ { } [ ] , $ = ! - # ( ) % . + ~ _ *

Sur les terminaux Windows, toute valeur de lettre suivie de deux points (par exemple, C:) est également prise en charge.

L'échappement de l'astérisque (*) n'est pas pris en charge pour le moment. Par exemple, vous ne pouvez pas l'utiliser pour exclure un fichier qui contient un astérisque dans son nom de fichier.

Lors de l'ajout d'exclusions DLL, les caractères génériques ne sont pas autorisés.

| Caractère générique | Description |
|---|---|
| * | Cela correspond à zéro ou plusieurs caractères, à l'exception des séparateurs de chemin d'accès aux fichiers spécifiques à la plateforme. Les séparateurs de chemin de fichier sont « \ » sur les terminaux Windows et « / » sur Linux et macOS. |
| ** | Cela correspond à zéro ou plusieurs répertoires dans un chemin absolu pour exclure des lecteurs, des répertoires et des répertoires enfants. Par exemple, `C:\MyApp\''\**\''`.<br>Suivez les règles ci-après lorsque vous utilisez le caractère générique `**` :<br>• Utilisez systématiquement `**` avec les séparateurs de chemin de fichier, tels que `\**\` ou `/**/`<br>• Le schéma `**\` est valide s'il se trouve au début du schéma pour les terminaux Windows uniquement. Il correspond à tous les répertoires de tous les lecteurs.<br>• Vous pouvez utiliser `\**\` ou `/**/` à plusieurs reprises dans un chemin, sans aucune limitation. |

**Remarque :** Dans un caractère générique normal, trois astérisques *** sont valides et correspondent à un seul astérisque *. Cependant, trois astérisques ne sont pas valides pour les exclusions car ils masqueraient les fautes de frappe. Par exemple, dans le modèle C:***.exe, les utilisateurs auraient peut-être voulu saisir C:***.exe mais

ont oublié de saisir un \. Si *** était traité comme un seul *, cela pourrait entraîner un comportement différent de celui prévu.

#### Exemples de caractères génériques Windows utilisés dans les exclusions de protection de la mémoire

Les exemples suivants sont basés sur l'exclusion d'un exécutable stocké dans le chemin suivant : `C:\Application\TestApp\MyApp\program.exe`

| | Exemples |
|---|---|
| Exemples de chemins d'exclusion valides | **Exclusion de chemin relatif sans caractères génériques** :<br>`\Application\TestApp\MyApp\program.exe`<br>**Exclure program.exe tant que program.exe est situé dans le répertoire « MyApp » dans C:\Application** :<br>`C:\Application\**\MyApp\program.exe`<br>**Exclure tout fichier .exe situé dans le répertoire « MyApp » dans C:\Application** :<br>`C:\Application\**\MyApp\*.exe`<br>**Exclure tout exécutable (quelle que soit son extension de fichier) tant qu'il se trouve dans le répertoire « MyApp » dans C:\Application** :<br>`C:\Application\**\MyApp\*`<br>**Exclure program.exe tant qu'il se trouve dans un répertoire enfant de C:\Application\TestApp** :<br>`C:\Application\TestApp\**\program.exe`<br>**Exclure program.exe tant qu'il se trouve dans \Application\TestApp\MyApp\ du lecteur C: :**<br>`C:\**\Application\TestApp\MyApp\program.exe`<br>**Exclure tout exécutable .exe tant qu'il se trouve dans \Application\TestApp\MyApp\ du lecteur C:** :<br>`C:\**\Application\TestApp\MyApp\*.exe`<br>**Exclure tout exécutable (quelle que soit son extension) tant qu'il se trouve à l'adresse \Application\TestApp\MyApp\ du lecteur C: :**<br>`C:\**\Application\TestApp\MyApp\*` |

| | Exemples |
|---|---|
| Utilisation incorrecte des astérisques dans les exclusions | Utilisez uniquement un astérisque (*) pour faire correspondre les caractères d'un nom de dossier ou de fichier. Les astérisques doubles (**) sont réservés pour correspondre aux chemins de répertoire et ne peuvent pas être utilisés à la fin d'une exclusion.<br>Voici une liste d'exemples dans le contexte de l'exclusion de `C:\Application\TestApp\MyApp\program.exe`.<br>• **Incorrect :** `C:\Application\TestApp\MyApp**.exe`<br>• **Incorrect :** `C:\Application**\MyApp\program.exe`<br>• **Correct :** `C:\Application\TestApp\MyApp\*.exe`<br>• **Correct :** `C:\Application\TestApp\*\*.exe`<br>• **Correct :**`C:\Application\**\program.exe` |
| Exclusions non recommandées | Évitez d'utiliser un double astérisque (**) immédiatement après une lettre de disque. Par exemple :<br>`C:\**\program.exe`<br>Dans cet exemple, `program.exe` est autorisé à s'exécuter à partir de n'importe quel dossier du lecteur `C:`. Bien que cette exclusion soit techniquement correcte, elle exclut tout élément dans n'importe quel répertoire (y compris les répertoires enfants) sur le lecteur. |

**Exemples de caractères génériques macOS utilisés dans les exclusions de protection de la mémoire**

Les exemples suivants sont basés sur l'exclusion d'un exécutable stocké dans le chemin suivant : `/Application/TestApp/MyApp/program.dmg`

| Type | Description |
|---|---|
| Utilisation correcte des exclusions | **Exclut program.dmg tant que program.dmg se trouve dans le répertoire enfant « MyApp »** :<br>`/Application/**/MyApp/program.dmg`<br>**Exclut tout exécutable avec .dmg tant qu'il est situé dans le répertoire enfant « MyApp »** :<br>`/Application/**/MyApp/*.dmg`<br>**Exclut tout exécutable tant qu'il se trouve dans le répertoire enfant « MyApp »** :<br>`/Application/**/MyApp/*`<br>**Exclut program.dmg tant qu'il se trouve dans un répertoire enfant du répertoire « TestApp »** :<br>`/Application/TestApp/**/program.dmg` |

| Type | Description |
| --- | --- |
| Utilisation incorrecte des astérisques dans les exclusions | Utilisez uniquement un astérisque (*) pour faire correspondre les caractères d'un nom de dossier ou de fichier. Les astérisques doubles (**) sont réservés pour correspondre aux chemins de répertoire et ne peuvent pas être utilisés à la fin d'une exclusion.<br>Voici une liste d'exemples dans le contexte de l'exclusion de `/Application/TestApp/MyApp/program.dmg`.<br>• • **Incorrect :** /Application/TestApp/MyApp/pro**am.dmg<br>• **Correct :** /Application/TestApp/MyApp/progra*.dmg<br>•<br>• • **Incorrect :** /Application/**<br>• **Correct :** /Application/**/* |
| Exclusions non recommandées | Évitez d'utiliser un double astérisque (**) au début d'une exclusion. Par exemple :<br>`/**/program.dmg`<br>Dans cet exemple, `program.dmg` est autorisé à s'exécuter à partir de n'importe quel dossier du lecteur. Bien que cette exclusion soit techniquement correcte, elle exclut tout élément dans n'importe quel répertoire (y compris les répertoires enfants) sur le lecteur. |

## Paramètres de protection

CylancePROTECT Desktop surveille toujours l'exécution de processus malveillants et alerte la console en cas de tentative d'exécution anormale ou dangereuse. Vous pouvez configurer l'agent CylancePROTECT Desktop à l'aide des paramètres suivants, disponibles dans l'onglet **Paramètres de protection** d'une stratégie de terminal.

| Option | Description |
| --- | --- |
| **Empêcher l'arrêt du service à partir du terminal** | Si cette option est sélectionnée, les utilisateurs du terminal ne peuvent pas arrêter le service pour l'agent CylancePROTECT Desktop ou pour les versions suivantes de l'agent CylanceOPTICS :<br>• Agent CylanceOPTICS pour Windows 3.1 ou version ultérieure avec CylancePROTECT Desktop 3.0 ou version ultérieure<br>• Agent CylanceOPTICS pour macOS 3.3 ou version ultérieure avec CylancePROTECT Desktop 3.1 ou version ultérieure<br>Lorsque ce paramètre est activé, un utilisateur macOS ne peut arrêter les services que si le niveau d'autoprotection dans les propriétés du terminal est défini sur Admin local (Actifs > Terminaux > cliquez sur le terminal). Les utilisateurs Windows ne peuvent pas arrêter les services de l'agent tant que ce paramètre est activé.<br>L'agent CylancePROTECT Desktop 3.1 et version ultérieure s'exécute en tant que service fiable à l'aide de la technologie AM-PPL (Antimalware Protected Process Light) de Microsoft, qui permet également d'empêcher l'arrêt de l'agent. Cette fonctionnalité nécessite que le terminal exécute Windows 10 1709 ou versions ultérieures ou Windows Server 2019 ou versions ultérieures. |

| Option | Description |
| --- | --- |
| **Arrêter les processus en cours d'exécution dangereux et leurs sous-processus** | Si ce paramètre est sélectionné, l'agent met fin aux processus et aux processus enfants (.exe ou .dll), quel que soit leur état lorsqu'une menace est détectée. Vous disposez ainsi d'un niveau de contrôle élevé sur les processus malveillants qui peuvent être en cours d'exécution sur un terminal.<br><br>Le fichier doit être mis en quarantaine automatiquement, manuellement ou à l'aide de la liste de quarantaine globale. Cette fonction doit être activée avant la mise en quarantaine du fichier. Si cette fonction est activée, mais que le fichier n'est pas mis en quarantaine ou qu'il est mis en quarantaine automatiquement, les processus continuent à s'exécuter.<br><br>**Exemple :** un fichier est autorisé à s'exécuter, puis vous décidez de le mettre en quarantaine. Lorsque ce paramètre est activé, le fichier est mis en quarantaine et le processus ainsi que tous les processus enfants sont interrompus. Si ce paramètre est désactivé, le fichier est mis en quarantaine, mais étant donné qu'il a été autorisé à s'exécuter, tous les processus démarrés par le fichier peuvent continuer à s'exécuter. |

| Option | Description |
| --- | --- |
| **Détection des menaces en arrière-plan** | Une analyse complète du disque est exécutée pour détecter et analyser les menaces inactives sur le disque. L'analyse complète du disque est conçue pour minimiser l'impact sur l'utilisateur final en utilisant peu de ressources système. L'analyse de détection des menaces en arrière-plan peut prendre jusqu'à une semaine, en fonction de l'activité du système et du nombre de fichiers du système qui doivent être analysés. Les date et heure de la dernière analyse d'arrière-plan terminée sont consignées dans la console.<br><br>Vous pouvez choisir d'exécuter l'analyse une seule fois lors de l'installation, ou de la planifier de manière récurrente à un intervalle spécifié. L'intervalle entre les analyses par défaut est de 10 jours. Une mise à niveau importante du modèle de détection, comme le fait d'ajouter de nouveaux systèmes d'exploitation, déclenche également une analyse complète du disque. Notez que l'augmentation de la fréquence des analyses peut avoir un impact sur les performances du terminal.<br><br>Il est recommandé d'activer le paramètre **Détection des menaces en arrière-plan** sur **Exécuter une fois** et d'activer **Contrôler les nouveaux fichiers** qui analyse les nouveaux fichiers et les fichiers mis à jour sur le disque. Si vous souhaitez contrôler des fichiers nouveaux et mis à jour, vous devez activer l'analyse de tous les fichiers existants une seule fois. En raison de la nature prédictive de la technologie, des analyses régulières de l'ensemble du disque ne sont pas requises, mais peuvent être implémentées à des fins de conformité (par exemple, la conformité PCI).<br><br>**Remarque :** Si des analyses de détection des menaces en arrière-plan sont exécutées simultanément sur plusieurs terminaux de machine virtuelle provenant du même hôte de machine virtuelle, les performances des terminaux en seront affectées. Envisagez d'activer cette fonction de manière incrémentielle pour les terminaux de machine virtuelle afin de limiter le nombre d'analyses effectuées simultanément.<br><br>Pour exécuter manuellement l'analyse, utilisez l'une des commandes suivantes :<br><br>• Sur les terminaux Windows :<br><br>`C:\Program Files\Cylance\Desktop\CylanceSvc.exe /backgroundscan`<br><br>• Sur les terminaux macOS :<br><br>`/Applications/Cylance/CylanceUI.app/Contents/MacOS/CylanceUI -background-scan`<br><br>• Sur les terminaux Linux :<br><br>`/opt/cylance/desktop/Cylance -b`<br>`/opt/cylance/desktop/Cylance --start-bg-scan` |

| Option | Description |
| --- | --- |
| **Contrôler les nouveaux fichiers** | Ce paramètre permet à l'agent d'analyser les fichiers nouveaux ou modifiés pour détecter les menaces dormantes. Si une menace est détectée, le fichier est mis en quarantaine même s'il n'y a pas eu de tentative d'exécution. Il est recommandé d'activer ce paramètre en même temps que la détection des menaces en arrière-plan (exécution unique).<br><br>Le mode de mise en quarantaine automatique (contrôle d'exécution) bloque les fichiers dangereux ou anormaux lors de l'exécution. Par conséquent, il n'est pas nécessaire d'activer l'option Contrôler les nouveaux fichiers lorsque le mode quarantaine automatique est également activé, sauf si vous préférez mettre en quarantaine un fichier malveillant dès que l'agent détecte la menace pendant une analyse.<br><br>Ce paramètre peut avoir un impact sur les performances. Envisagez de surveiller les performances de traitement des disques ou des messages pour voir si elles ont changé. L'exclusion de dossiers spécifiques peut améliorer les performances et garantir que certains dossiers et fichiers ne seront pas analysés par l'agent. |
| **Définir la taille maximale du fichier d'archive à analyser** | Spécifiez la taille maximale du fichier d'archive que l'agent doit analyser. Ce paramètre s'applique à **Détection des menaces en arrière-plan** et à **Contrôler les nouveaux fichiers**. Si vous ne souhaitez pas analyser les fichiers d'archive, définissez la taille du fichier sur 0 Mo. |

| Option | Description |
| --- | --- |
| **Exclure des dossiers spécifiques** | Ce paramètre vous permet de spécifier les dossiers et sous-dossiers que vous souhaitez exclure de l'analyse via les fonctions **Détection des menaces en arrière-plan** et **Contrôler les nouveaux fichiers**.<br><br>Pour Windows, utilisez un chemin absolu avec la lettre du lecteur. Par exemple, `C:\Test`.<br><br>Pour macOS , utilisez un chemin absolu à partir de la racine sans la lettre de lecteur. Par exemple, `/Applications/SampleApplication.app`.<br><br>Pour Linux , utilisez un chemin absolu à partir de la racine sans la lettre de lecteur. Par exemple, `/opt/application`.<br><br>**Exemple pour Windows** : `C:\Test`<br><br>**Exemple pour macOS (sans espaces)** : `/Applications/SampleApplication.app`<br><br>**Exemple pour macOS (avec espaces)** : `/Applications/Sample\ Application.app`<br><br>**Exemple pour Linux** : `/opt/application/`<br><br>Le caractère générique * est également pris en charge pour les exclusions de dossiers. Pour plus d'informations, reportez-vous à Caractères génériques dans les exclusions du dossier des paramètres de protection.<br><br>Les exclusions ne sont pas appliquées de manière rétroactive. Après l'installation initiale de l'agent, les fonctionnalités Détection des menaces en arrière-plan et Contrôler les nouveaux fichiers ignorent les fichiers en fonction de la liste d'exclusion reçue. L'ajout d'une exclusion après la détection ou l'imputation initiale n'exclura pas rétroactivement les fichiers déjà détectés ou réputés dangereux. Tous les fichiers précédemment détectés ou réputés dangereux resteront dans cet état jusqu'à ce qu'ils soient localement dispensés ou ajoutés à la liste sécurisée globale.<br><br>Par exemple, si l'option Contrôler les nouveaux fichiers impute un fichier appelé C:\Windows\ccmcache\test.exe et qu'une exclusion est ajoutée ultérieurement à l'onglet Paramètres de protection pour C:\Windows\ccmcache\, le fichier réputé dangereux restera réputé dangereux même si le dossier a été ajouté comme exclusion Dans ce cas, il restera réputé dangereux jusqu'à ce que vous renonciez au fichier localement ou que vous l'ajoutiez à la liste sécurisée globale. |
| **Autoriser l'exécution** | Les fichiers exécutés à partir de n'importe quel dossier sont soumis au contrôle d'exécution/à la mise en quarantaine automatique, même s'ils sont spécifiés dans Exclure des dossiers spécifiques. Vous pouvez activer le paramètre Autoriser l'exécution pour permettre l'exécution de fichiers à partir de dossiers spécifiés dans la liste Exclure des dossiers spécifiques. Ce paramètre s'applique à tous les dossiers de la liste, et pas seulement au premier ou au dernier élément saisi.<br><br>Les fichiers et mes menaces déplacés vers ces dossiers seront autorisés à s'exécuter et pourraient compromettre votre terminal et votre organisation. Prenez les précautions nécessaires pour vous assurer que les fichiers non autorisés ne peuvent pas être ajoutés aux dossiers exclus. |

| Option | Description |
| --- | --- |
| **Copier les exemples de fichier (logiciels malveillants)** | Spécifiez un lecteur réseau partagé pour stocker des copies des échantillons de fichiers trouvés via les fonctionnalités Détection des menaces en arrière-plan, Contrôler les nouveaux fichiers et Contrôler l'exécution. Cela vous permet d'effectuer votre propre analyse des fichiers que CylancePROTECT Desktop considère comme dangereux ou anormaux.<br>• Les partages réseau CIFS/SMB sont pris en charge.<br>• Spécifiez un emplacement de partage réseau. Vous devez utiliser un chemin complet. Exemple : `\\server_name\shared_folder`.<br>• Tous les fichiers répondant aux critères sont copiés sur le partage réseau, même s'il s'agit de doublons. Aucun test d'unicité n'est réalisé.<br>• Les fichiers sont compressés.<br>• Les fichiers sont protégés par mot de passe. Le mot de passe est « infecté ». |

#### Caractères génériques dans les exclusions du dossier des paramètres de protection

Vous pouvez utiliser l'astérisque (*) comme caractère générique pour tous les systèmes d'exploitation lorsque vous spécifiez des exclusions de dossiers dans l'onglet **Paramètres de protection**.

| Caractère | Signification |
| --- | --- |
| * | Utilisez l'astérisque pour exclure des dossiers et pour représenter un préfixe ou un suffixe pour un nom de dossier.<br>• L'astérisque correspond à un ou plusieurs caractères, à l'exception du séparateur de chemin spécifique à la plateforme (« \ »).<br>• Plusieurs caractères génériques sont autorisés dans un chemin d'exclusion.<br>• Pour le moment, l'échappement * n'est pas pris en charge. Par exemple, vous ne pouvez pas exclure un dossier qui contient un astérisque « * » dans le nom du dossier.<br>• La fonctionnalité d'exclusion de dossier précédente s'applique toujours. Cela signifie que des exclusions s'appliqueront également à tous les dossiers enfants. |

| Caractère | Signification |
| --- | --- |
| Exemples d'exclusions de dossiers | Voici quelques exemples d'exclusion de `C:\Application\TestFolder1\MyApp\program.exe`.<br>**Exemples d'utilisation correcte des caractères génériques dans les exclusions de dossiers**<br>• Une exclusion sans caractères génériques.<br>`C:\Application\TestFolder1\MyApp\`<br>• Un caractère de remplacement est utilisé pour spécifier un dossier parent du dossier « MyApp ».<br>C:\Application*\MyApp\<br>• Un caractère générique est utilisé pour spécifier qu'il y a un préfixe (c'est-à-dire « Test ») dans le nom du dossier pour que l'agent puisse faire une comparaison.<br>C:\Application*Folder1\MyApp\<br>• Un caractère générique est utilisé pour spécifier qu'il existe un suffixe (c'est-à-dire « 1 ») dans le nom du dossier pour que l'agent puisse faire une comparaison.<br>C:\Application\TestFolder*\MyApp\<br>• Un caractère générique est utilisé pour spécifier qu'il y a un préfixe (c'est-à-dire « Test ») et un suffixe (c'est-à-dire « 1 ») dans le nom du dossier pour que l'agent puisse faire une comparaison.<br>C:\Application*Folder*\MyApp\<br>• Un caractère générique est utilisé pour exclure tous les dossiers sous « Application » dans le lecteur C.<br>C:\Application*\<br>• Un caractère de remplacement est utilisé pour exclure tous les dossiers sous « Application » pour tous les lecteurs.<br>*\Application*\<br>**Exemples d'utilisation incorrecte des caractères génériques dans les exclusions de dossiers**<br>• `C:\Application\TestFolder1\MyApp\*.exe`<br>Un caractère générique ne peut pas être utilisé dans le nom de fichier d'un exécutable. Utilisez des caractères génériques pour les noms de dossier ou de répertoire uniquement.<br>• C:\Application**<br>Les astérisques doubles (**) ne sont pas pris en charge dans les exclusions de dossiers. Utilisez plutôt un astérisque (*).<br>**Exclusions de dossiers non recommandées**<br>`C:\*`<br>Bien que cette exclusion soit une entrée valide, elle exclurait effectivement tout ce qui se trouve dans n'importe quel répertoire (y compris les répertoires enfants) de l'ensemble du lecteur C:. |

## Contrôle d'applications

Le contrôle des applications est un paramètre facultatif qui permet aux utilisateurs de limiter toute modification apportée aux fichiers exécutables sur les terminaux Windows et Linux. Seules les applications installées sur le terminal avant l'activation du contrôle d'applications sont autorisées à s'exécuter. En général, le contrôle des applications est utilisé pour les terminaux à fonction fixe qui ne sont pas modifiés après leur mise en place (par exemple, les terminaux de point de vente).

Lorsque le contrôle des applications est activé, les tentatives d'ajout d'applications et de modification d'applications sur le terminal sont refusées. Cela signifie que les applications ne peuvent pas être téléchargées à partir de navigateurs Web ni copiées à partir d'un autre terminal ou ordinateur (tel qu'un lecteur externe ou partagé).

Le contrôle d'applications poursuit les principaux objectifs suivants :

- Refuser l'exécution de fichiers exécutables à partir de lecteurs distants ou externes
- Refuser la création de nouveaux fichiers exécutables sur le disque local
- Refuser les modifications apportées aux fichiers existants sur le disque local

Tenez compte des points suivants lors de l'utilisation du contrôle d'applications :

- Le processus de mise à jour des agents CylancePROTECT Desktop et CylanceOPTICS est désactivé lorsque le contrôle d'applications est activé.
- Vous ne pouvez pas supprimer CylancePROTECT Desktop et l'agent CylanceOPTICS lorsque le contrôle d'applications est activé.
- Il est déconseillé d'exécuter CylanceOPTICS sur des systèmes utilisant le contrôle d'applications. Lorsque le contrôle d'applications est activé, CylanceOPTICS ne fonctionne pas correctement en raison de la nature restrictive du contrôle d'applications.
- L'exécution de tous les fichiers exécutables sur des lecteurs externes ou distants est refusée lorsque le contrôle des applications est activé. Pour éviter les pannes de production ou l'activité excessive du réseau, le contrôle des applications ne surveille pas les transferts de fichiers vers des disques distants ou externes.
- Consultez Considérations relatives à l'utilisation du contrôle des applications sur les terminaux Linux.

#### Paramètres de contrôle d'application

| Option | Description |
|---|---|
| **Contrôle d'applications** | Ce paramètre indique s'il faut activer le contrôle des applications. Lorsque vous activez le contrôle d'applications, les paramètres recommandés suivants sont automatiquement appliqués :<br>• Dans l'onglet **Actions sur les fichiers**, les paramètres **Mise en quarantaine automatique avec contrôle d'exécution** sont sélectionnés pour les fichiers non sécurisés et anormaux.<br>• Dans l'onglet **Actions de mémoire**, le paramètre **Protection de la mémoire** est sélectionné. Tous les types de violation de la protection de la mémoire seront définis sur **Terminer**.<br>• Dans l'onglet **Paramètres de protection**, le paramètre **Contrôler les nouveaux fichiers** est sélectionné.<br>Si vous souhaitez modifier l'un de ces paramètres, effacez la sélection dans les onglets spécifiés. |

| Option | Description |
| --- | --- |
| **Modifier la fenêtre** | Lorsqu'il est activé, ce paramètre désactive temporairement le contrôle d'applications pour permettre la modification et l'exécution de nouvelles applications ou pour effectuer des mises à jour, y compris la mise à jour de l'agent. Après avoir effectué les modifications nécessaires, décochez cette case pour fermer la fenêtre de modification et réactiver le contrôle de l'application.<br>Lorsque vous utilisez ce paramètre pour désactiver temporairement le contrôle d'applications, les modifications telles que les exclusions de dossiers sont conservées. Si vous désactivez le paramètre **Contrôle d'applications**, les paramètres sont réinitialisés sur les valeurs par défaut. |
| **Exclusions de dossiers (y compris les sous-dossiers)** | Ce paramètre spécifie un chemin absolu de dossiers autorisés à apporter des modifications et des ajouts à l'application lorsque le contrôle de l'application est activé. Ce paramètre s'applique aux terminaux exécutant l'agent Windows 1410 ou versions ultérieures.<br>Exemple : `C:\Program Files\Microsoft SQL Server`<br>Les exclusions de dossiers ne sont disponibles que pour les lecteurs internes locaux. Les exclusions pour les lecteurs amovibles ou distants ne sont pas prises en charge. |

#### Afficher l'activité de contrôle d'applications

Vous pouvez trouver l'activité de contrôle d'applications d'un terminal à partir de sa page **Détails du terminal** dans la section **Menaces et activités**.

#### Considérations relatives à l'utilisation du contrôle des applications sur les terminaux Linux

Tenez compte des points suivants avant d'activer le contrôle d'application dans une stratégie de terminal pour les terminaux Linux :

- Les exclusions de dossiers dans la stratégie de contrôle de l'application ne sont pas prises en charge par l'agent Linux.
- Lorsque le contrôle d'applications est activé, un inventaire de tous les fichiers exécutables sur le système de fichiers local est généré. L'exécution des fichiers est limitée aux fichiers de l'inventaire.
- Les fichiers exécutables peuvent être ajoutés au terminal une fois le contrôle de l'application activé, mais ils ne peuvent pas être exécutés. Seules les applications faisant partie de l'inventaire lorsque le contrôle d'applications est activé sont autorisées à s'exécuter.
- Autoriser une mise à jour sur un terminal Linux où le contrôle d'applications est activé peut entraîner des problèmes.

## Paramètres de l'agent

Utilisez les paramètres de l'agent pour afficher les notifications sur le bureau lorsque des opérations telles que la mise en quarantaine d'un fichier a lieu sur des terminaux. Vous pouvez également charger les fichiers journaux de l'agent sur la console à partir de cette page.

| Option | Description |
| --- | --- |
| **Activer le chargement automatique des fichiers journaux** | Activez le chargement automatique des journaux de l'agent et affichez-les dans la console. Les fichiers journaux chargés sont stockés pendant 30 jours.<br>Après l'activation de cette option, un onglet Journaux de l'agent s'affiche lorsque vous sélectionnez un terminal attribué à cette stratégie dans l'onglet Terminaux. Le nom du fichier journal est la date du journal. |
| **Activer les notifications de bureau** | Les fenêtres contextuelles de notification d'agent peuvent être configurées sur chaque terminal ou au niveau de la stratégie dans la console. L'activation ou la désactivation des fenêtres contextuelles de notification d'agent au niveau du terminal est prioritaire sur les paramètres de la console. Assurez-vous que le terminal pour lequel vous souhaitez obtenir les fichiers journaux est attribué à cette stratégie.<br>Dans l'interface utilisateur de l'agent, l'onglet Événements est effacé si CylanceUI ou le terminal est redémarré. |
| **Activer l'inventaire logiciel** | Ce paramètre spécifie si l'agent envoie à la console de gestion une liste des applications installées sur les terminaux. Cette fonctionnalité permet aux administrateurs d'identifier les applications installées sur les terminaux qui peuvent être une source de vulnérabilités, de hiérarchiser les actions contre les vulnérabilités et de les gérer en conséquence.<br>Pour utiliser cette fonctionnalité, vous devez disposer de CylancePROTECT Desktop pour Windows version 3.2.<br>Vous pouvez afficher la liste de toutes les applications installées sur les terminaux enregistrés auprès du locataire à partir de l'écran **Actifs > Applications installées** et, pour chaque application, la liste des terminaux sur lesquels elle est installée. Vous pouvez également afficher la liste des applications installées sur des terminaux individuels à partir de l'écran **Actifs > Terminaux > Détails du terminal > Applications installées**. |

## Contrôle de script

Le contrôle de script protège les terminaux Windows en empêchant l'exécution de scripts. Si vous souhaitez autoriser l'exécution de scripts, vous pouvez ajouter des exclusions de plusieurs façons à l'aide de caractères génériques. Par exemple, vous pouvez configurer la règle pour empêcher l'exécution des scripts et autoriser uniquement l'exécution des scripts ajoutés à la liste d'exclusion.

| Élément | Description |
| --- | --- |
| Action | Pour chaque type de script, vous pouvez sélectionner l'une des actions suivantes :<br>• **Désactivé** : cette action permet d'exécuter tous les scripts, mais ne les signale pas à la console. Ce paramètre est déconseillé.<br>• **Alerte** : cette action permet d'exécuter tous les scripts et les signale à la console. Utilisez ce paramètre lorsque vous souhaitez surveiller et observer tous les scripts en cours d'exécution dans votre environnement. Ce paramètre est recommandé pour le déploiement initial lorsque vous déterminez les scripts que vous souhaitez autoriser ou bloquer.<br>• **Bloquer** : cette action empêche l'exécution de tous les scripts et les signale à la console. Seuls les fichiers ajoutés à la liste d'exclusion sont autorisés à s'exécuter. Utilisez ce paramètre après avoir testé et contrôlé les menaces en mode alerte.<br>Les réglages suivants sont disponibles pour les paramètres Script actif et Script PowerShell :<br>• **Bloquer les scripts dangereux** : si le script ne figure pas déjà dans la liste d'exclusion, CylancePROTECT reçoit un indice de menace pour le script provenant des services cloud Cylance et, s'il s'agit d'un indice de menace dangereuse, l'exécution du script est bloquée. Les fichiers dangereux ressemblent beaucoup à des logiciels malveillants. Les scripts non notés et anormaux sont signalés sur la console, mais ils ne sont pas bloqués.<br>• **Bloquer les scripts anormaux et dangereux** : si le script ne figure pas dans la liste d'exclusion, CylancePROTECT reçoit un indice de menace pour le script provenant des services cloud Cylance et, s'il s'agit d'un indice de menace anormale ou dangereuse, l'exécution du script est bloquée. Les fichiers dangereux ressemblent beaucoup à des logiciels malveillants. Les fichiers anormaux présentent des attributs semblables à ceux d'un logiciel malveillant, mais sont moins susceptibles d'être des logiciels malveillants qu'un fichier dangereux. Les scripts non notés sont signalés sur la console, mais ils ne sont pas bloqués.<br>Vous pouvez trouver des évènements d'alerte et de bloc de contrôle de script dans l'écran **Protection > Contrôle de script**. |
| **Script actif** | Ce paramètre détermine si vous souhaitez autoriser l'exécution des scripts actifs ou les bloquer. Les scripts actifs incluent VBScript et JScript<br>Pour renforcer le contrôle des scripts, utilisez l'un des paramètres **Bloquer les scripts dangereux** ou **Bloquer les scripts anormaux et dangereux**. Ces paramètres nécessitent l'agent CylancePROTECT Desktop 3.2 ou version ultérieure. Si un terminal exécute un agent de version antérieure, le script est bloqué par défaut. |

| Élément | Description |
| --- | --- |
| **Script PowerShell** | Ce paramètre détermine si vous souhaitez autoriser ou bloquer l'exécution des scripts PowerShell.<br><br>Pour renforcer le contrôle des scripts, utilisez l'un des paramètres **Bloquer les scripts dangereux** ou **Bloquer les scripts anormaux et dangereux**. Ces paramètres nécessitent l'agent CylancePROTECT Desktop 3.2 ou version ultérieure. Si un terminal exécute un agent de version antérieure, le script est bloqué par défaut. |
| **Console PowerShell** | Ce paramètre détermine si vous souhaitez autoriser l'exécution de la console PowerShell ou bloquer son lancement. Le blocage de la console PowerShell fournit une sécurité supplémentaire en empêchant son utilisation en mode interactif.<br><br>Le mode alerte pour la console PowerShell nécessite l'agent CylancePROTECT Desktop 3.2 ou version ultérieure. Il permet l'exécution de scripts et signale l'évènement détecté à la console de gestion. Pour les agents qui ne prennent pas en charge le mode alerte, l'utilisation de la console PowerShell est autorisée par défaut et aucune alerte n'est générée.<br><br>Si vous utilisez un script qui lance la console PowerShell, mais que celle-ci est bloquée, le script échoue. Si possible, il est recommandé aux utilisateurs de modifier leurs scripts pour appeler les scripts PowerShell, et non la console PowerShell. Pour cela, vous pouvez utiliser le commutateur `-file`. Une commande de base pour exécuter un script PowerShell sans appeler la console serait la suivante : `Powershell.exe -file [script name]` |

| Élément | Description |
| --- | --- |
| **Macros** (2.1.1578 et versions antérieures) | Ce paramètre détermine s'il faut alerter ou bloquer les macros Microsoft Office. Les macros utilisent Visual Basic for Applications (VBA) qui permet d'incorporer du code à l'intérieur d'un document Microsoft Office (comme Microsoft Office, Excel et PowerPoint). L'objectif principal des macros est de simplifier les actions de routine, telles que la manipulation des données dans une feuille de calcul ou le formatage du texte dans un document. Cependant, les créateurs de programmes malveillants peuvent utiliser des macros pour exécuter des commandes et attaquer le système. On suppose qu'une macro effectue une action malveillante lorsqu'elle tente de manipuler le système. L'agent recherche les actions malveillantes provenant d'une macro qui affecte des éléments extérieurs aux produits Microsoft Office.<br><br>Tenex compte des remarques suivantes :<br>• La fonctionnalité de macros de contrôle de script fonctionne avec l'agent 2.1.1578 et les versions antérieures. Pour les agents plus récents, utilisez le type de violation **Macros VBA dangereuses** avec stratégie de protection de la mémoire.<br>• Toute exclusion de macro créée pour le contrôle de script doit être ajoutée aux exclusions de protection de la mémoire pour le type de violation **Macros VBA dangereuses**.<br>• À partir de Microsoft Office 2013, les macros sont désactivées par défaut. La plupart du temps, vous n'avez pas besoin d'activer les macros pour afficher le contenu d'un document Microsoft Office. Vous ne devez activer les macros que pour les documents que vous recevez d'utilisateurs de confiance, et vous avez une bonne raison de les activer. Sinon, les macros doivent toujours être désactivées. |
| **Python** | Ce paramètre détermine si les scripts Python (versions 2.7 et 3.0 à 3.8) doivent être autorisés ou s'ils doivent être bloqués. Ce paramètre est valide pour l'agent 2.1.1580 ou version ultérieure. |
| **.NET DLR** | Ce paramètre détermine si les scripts DLR .NET doivent être exécutés ou s'ils doivent être bloqués. Ce paramètre est valide pour l'agent 2.1.1580 ou version ultérieure. |

| Élément | Description |
| --- | --- |
| **Macros XLM** (préversion) | **Remarque :** La fonctionnalité des macros XLM est actuellement disponible en mode Préversion, où elle peut se comporter de manière inattendue.<br><br>Ce paramètre détermine si CylancePROTECT Desktop autorise les macros Excel 4.0 (XLM) à être exécutées ou non. Lorsque les macros sont activées et exécutées, l'interface AMSI de Microsoft communique avec l'agent pour déterminer si la macro doit être exécutée ou si elle doit être bloquée conformément à la stratégie de terminal.<br><br>Cette fonctionnalité requiert les éléments suivants :<br><br>• Microsoft Windows 10 ou versions ultérieures<br>• Agent de CylancePROTECT Desktopversion 3.1<br>• Les macros VBA doivent être désactivées dans le menu Excel **Fichier > Centre de gestion de la confidentialité > Centre de gestion de la confidentialité Excel > Paramètres des macros**. |
| **Paramètres avancés** | Les paramètres avancés suivants encouragent l'évaluation des scripts et tirent parti du contrôle de script :<br><br>• **Noter tous les scripts** : ce paramètre garantit que tous les scripts sont évalués, quel que soit le paramètre de contrôle de script. Par défaut, si le paramètre de contrôle de script est défini sur Alerte ou Bloquer, les scripts ne sont pas notés.<br>• **Charger le script dans le cloud** : ce paramètre spécifie si une copie du script est chargée vers les services cloud CylancePROTECT à des fins d'analyse et d'évaluation des menaces. Si cette option n'est pas sélectionnée, CylancePROTECT tente d'obtenir un indice pour le script à l'aide de ses informations de hachage.<br>• **Alerte en cas d'exécution de scripts suspects uniquement** : lorsqu'un script est évalué et qu'aucune menace n'est détectée, ce paramètre spécifie que l'exécution du script n'est pas signalée à la console de gestion. Si cette option n'est pas sélectionnée, l'exécution des scripts est signalée à la console de gestion, même si une menace n'est pas détectable. |

| Élément | Description |
| --- | --- |
| Exclure les fichiers, scripts ou processus | Vous pouvez spécifier des dossiers pour autoriser l'exécution de n'importe quel script de ce dossier (et de ses sous-dossiers) sans générer d'alerte même lorsque les contrôles de script sont réglés sur le blocage. Vous pouvez également ajouter des exclusions pour les processus afin de permettre l'exécution correcte des scripts de certaines applications qui seraient autrement bloqués. Par exemple, si le service informatique utilise des outils spécifiques pour exécuter des scripts en permanence, vous pouvez ajouter le processus de cet outil en tant qu'exclusion afin que des scripts puissent être exécutés via cet outil.<br><br>Spécifiez le chemin relatif du dossier ou du sous-dossier. Les chemins d'accès aux dossiers peuvent correspondre à un lecteur local, à un lecteur réseau mappé ou à un chemin d'accès de type UNC (Universal Naming Convention).<br><br>**Exclusion de dossiers et de scripts**<br><br>• Les exclusions de dossiers ne peuvent pas contenir le nom du script ou du fichier de macro. Ces entrées ne sont pas valides et l'agent les ignore.<br>• Si vous souhaitez exclure un script spécifique, vous devez utiliser un caractère générique. Pour plus d'informations sur la manière d'utiliser les caractères génériques pour exclure des scripts spécifiques, consultez Caractères génériques dans les exclusions du contrôle de script.<br>• Si le groupe « Tout le monde » de votre organisation a des droits d'écriture sur un dossier, n'importe qui à l'intérieur ou à l'extérieur de l'organisation peut déposer un script dans le dossier et y écrire. CylancePROTECT Desktop continuera à envoyer des alertes sur les scripts et à les bloquer. Les autorisations écrites s'appliquent non seulement au dossier parent direct, mais également à tous les dossiers parents, jusqu'à la racine.<br><br>**Exclusion de processus**<br><br>• Les exclusions de processus nécessitent l'agent version 2.1.1580 ou ultérieure.<br>• L'exécutable de l'exclusion du processus peut être mis en quarantaine par le contrôle d'exécution et donc bloqué. Si l'exécutable est mis en quarantaine, vous devez l'ajouter à la **Liste sécurisée des stratégies** dans l'onglet **Actions de fichier**.<br>• Les exclusions de processus continuent d'autoriser l'exécution des scripts et ne les empêchent pas de s'exécuter à partir du dossier spécifié. |

#### Caractères génériques dans les exclusions du contrôle de script

Vous pouvez utiliser l'astérisque (*) comme caractère générique lorsque vous spécifiez des exclusions dans l'onglet **Contrôle de script**.

Utiliser des caractères génériques dans les exclusions du contrôle de script réduit le nombre d'alertes affichées dans votre console tout en permettant aux utilisateurs d'exécuter certains scripts qui correspondent au chemin d'exclusion et au nom de fichier. Par exemple, vous pouvez exclure un script spécifique en employant son

nom complet lorsque vous utilisez un caractère générique dans le chemin d'accès au répertoire, ou recourir au caractère générique pour mettre en correspondance un groupe de scripts qui partagent un nom similaire en l'utilisant comme partie du nom de fichier proprement dit.

Bien que l'utilisation de caractères génériques dans les exclusions offre une certaine flexibilité, elle peut également réduire votre position de sécurité si vos exclusions sont trop larges. Par exemple, évitez d'exclure des dossiers complets tels que `/windows/temp`. Utilisez plutôt un caractère générique lorsque vous spécifiez le nom de fichier complet ou partiel du script que vous souhaitez exclure (par exemple, `/windows/temp/myscript*.vbs`).

Le tableau suivant décrit les règles des exclusions de contrôle de script :

| Élément | Description |
|---|---|
| Caractères génériques pris en charge | Seul l'astérisque (*) est pris en charge comme caractère générique pour les exclusions de contrôle de script.<br>Le caractère générique représente un ou plusieurs caractères. |
| Barres obliques de style UNIX | Si vous utilisez des caractères génériques, les exclusions doivent utiliser des barres obliques de type Unix (même pour les systèmes Windows).<br>Exemple : `/windows/system*/*` |
| Exclusions de dossiers | Lorsque vous souhaitez exclure un dossier, l'exclusion doit avoir un caractère générique à la fin du chemin pour distinguer l'exclusion en tant que dossier (et non en tant que fichier).<br>Par exemple :<br>• `/windows/system32/*`<br>• `/windows/*/test/*`<br>• `/windows/system32/test*/*` |
| Exclusions de fichiers | Lorsque vous souhaitez exclure un fichier, l'exclusion doit se terminer par une extension de fichier pour distinguer l'exclusion en tant que fichier (et non en tant que dossier). Par exemple :<br>• `/windows/system32/*.vbs`<br>• `/windows/system32/script*.vbs`<br>• `/windows/system32/*/script.vbs`<br>• Chaque caractère générique représente un seul niveau de dossier. Le nombre de niveaux de dossiers représentés dans l'exclusion doit correspondre au niveau du fichier que vous essayez d'exclure.<br>  • Par exemple, /folder/*/script.vbs correspond à \folder\test\script.vbs, mais pas à \folder\test\001\script.vbs. Cela nécessite /folder/*/001/script.vbs ou /folder/*/*/script.vbs.<br>  • Le caractère générique doit être conservé à chaque niveau jusqu'à l'emplacement du script.<br>  • Deux caractères génériques ou plus par niveau ne sont pas autorisés. Par exemple, /folder/*file*.ext n'est pas autorisé. |

| Élément | Description |
| --- | --- |
| Exclusions de processus | Les exclusions de processus avec un caractère générique doivent avoir une extension de fichier pour la distinguer comme une exclusion de processus (et non un dossier).<br>Pour spécifier un processus quel que soit le répertoire dans lequel il se trouve, reportez-vous aux exemples suivants :<br>• `/my*.exe` (lecteur local)<br>• `//my*.exe` (lecteur réseau)<br>Pour spécifier un processus qui se trouve dans un répertoire spécifique, reportez-vous aux exemples suivants :<br>• `/directory/child/my*.exe` (lecteur local)<br>• `//directory/child/my*.exe` (lecteur réseau) |
| Exemples de correspondances complètes et partielles dans les exclusions | Les caractères génériques prennent en charge les exclusions complètes et partielles.<br>• `/folder/*/script.vbs`<br>• `/folder/test*/script.vbs` |
| Chemins absolus | Les chemins absolus ne sont pas pris en charge dans les exclusions de contrôle de script. |
| Chemins relatifs | Si vous pouvez identifier un chemin relatif commun, vous pouvez exclure les chemins UNC (Universal Naming Convention) avec un caractère générique.<br>Par exemple, si vous utilisez des noms de terminal dans un chemin tel que « DC01 » à « DC24 » : `/dc*/path/to/script/*` |
| Chemins réseau | Les chemins réseau peuvent être exclus. Par exemple :<br>• `//hostname/application/*`<br>• `//host*/application/*`<br>• `//*name/*/application/*`<br>• `//hostname/*` |

**Exemples d'exclusions du contrôle de script**

L'ajout d'exclusions pour les scripts dynamiques exécutés à partir d'un emplacement de répertoire spécifique ou pour un script exécuté à partir de plusieurs dossiers d'utilisateurs différents est possible en utilisant des caractères génériques dans les exclusions de contrôle de script. Par exemple, vous pouvez utiliser le jeton * dans le chemin d'exception pour vous assurer qu'il couvre vos variantes.

Le tableau suivant inclut quelques exemples d'exclusions avec des correspondances qui seraient exclues avec succès et des non-correspondances qui ne seront pas exclues.

| Exemple d'exclusion | Correspondances | Non-correspondances |
|---|---|---|
| `/users/*/temp/*` | • `\users\john\temp`<br>• `\users\jane\temp` | • `\users\folder\john\temp`<br>• `\users\folder\jane\temp`<br>Ces dossiers ne seront pas exclus, car le nombre de niveaux de dossiers ne correspond pas. |
| `/program files*/app/script*.vbs` | • `\program files(x86)\app\script1.vbs`<br>• `\program files(x64)\app\script2.vbs`<br>• `\program files(x64)\app\script3.vbs` | • `\program files(x86)\app\script.vbs`<br>• `\program files\app\script1.vbs`<br>Ces dossiers ne seront pas exclus, car les caractères génériques représentent un ou plusieurs caractères. |
| `//*example.local/sysvol/script*.vbs` | `\\ad.example.local\sysvol\script1.vbs` | `\\ad.example.local\sysvol\script.vbs`<br>Ce script ne sera pas exclu, car les caractères génériques représentent un ou plusieurs caractères. |
| `/users/*/*/*.vbs` | • `/users/john/temp/script.vbs`<br>• `/users/john/temp/anotherscript.vbs` | • `/users/john/temp1/temp2/script.vbs`<br>Ce script ne sera pas exclu, car le nombre de niveaux de dossier ne correspond pas. |

**Exclusion de processus**

Vous pouvez ajouter des processus à la liste des exclusions de contrôle de script. Cette fonctionnalité peut être utile si vous souhaitez exclure des processus spécifiques qui peuvent appeler des scripts. Par exemple, vous pouvez exclure SCCM pour lui permettre de lancer des scripts PowerShell dans un répertoire temporaire. Un processus est tout ce qui appelle un interpréteur de script pour exécuter un script.

- L'exemple suivant permet au processus myfile.exe d'appeler un interpréteur (tel que PowerShell.exe) pour exécuter un script.
  - /windows/*/myfile.exe
- Les exemples suivants ajoutent myprocess.exe à la liste d'exclusion afin qu'il puisse s'exécuter quel que soit son chemin d'accès au dossier :
  - `\myprocess.exe` (sur un lecteur Windows local)
  - `\\myprocess.exe` (sur un lecteur Windows réseau)
- L'exemple suivant ajoute myprocess.exe à la liste d'exclusion afin qu'il ne puisse être exécutée qu'à partir d'un chemin de dossier spécifique :
  - `\directory\child\myprocess.exe` (sur un lecteur Windows local)
  - `\\directory\child\myprocess.exe` (sur un lecteur Windows réseau)

**Remarque :**

- Les chemins absolus ne sont pas pris en charge pour les exclusions.
- Les ancêtres ne sont pas pris en charge.
- Lorsqu'un fichier exécutable (exe) est ajouté à une exclusion, /[CySc_process]/ est automatiquement ajouté à l'exclusion. Si vous avez ajouté l'exemple d'exclusion ci-dessus, le résultat serait : /[CySc_process]/ /windows/*/myfile.exe.

**Options alternatives pour les exclusions de contrôle de script**

Vous pouvez utiliser la liste sécurisée globale ou ajouter un certificat comme méthode alternative pour exclure des scripts.

- Ajouter un fichier à la liste de quarantaine globale ou à la liste sécurisée globale de CylancePROTECT Desktop
  - Cette méthode nécessite une valeur de hachage SHA256 et suppose que cette valeur ne changera pas. Les mises à jour du script ou les modifications apportées par le script par conception entraînent la modification de la valeur de hachage. Par conséquent, cette méthode nécessite davantage de tâches administratives à maintenir si le script ou la macro est fréquemment mis à jour ou si elle change par programmation (par exemple, ajoute une nouvelle date ou heure, ou effectue des demandes système, extrait des données). Chaque fois que l'agent CylancePROTECT Desktop signale un script à la console de gestion, il doit indiquer une valeur de hachage SHA256. Chaque fois que la valeur de hachage change, l'agent signale la nouvelle valeur et vous devez ajouter la nouvelle valeur à la liste de sécurité globale. Si une valeur de hachage ne peut pas être générée (par exemple, si le script ne s'exécute pas correctement, si le fichier n'existe pas ou s'il y a des problèmes d'autorisation), un hachage générique est utilisé lorsque le script est signalé à la console.
  - La valeur de hachage SHA256 suivante est une valeur de hachage générique que l'agent de CylancePROTECT Desktop utilise lorsqu'un hachage ne peut pas être généré pour un script. Si vous essayez d'ajouter cette valeur à la liste de sécurité globale, un message d'erreur s'affiche en raison de la fonctionnalité de l'agent.
    - `FE9B64DEFD8BF214C7490AA7F35B495A79A95E81F8943EE279DC99998D3D3440`
  - La valeur de hachage SHA256 suivante est une valeur de hachage générique que l'agent CylancePROTECT Desktop utilise lorsqu'une ligne unique PowerShell est utilisée et qu'un hachage ne peut pas être généré pour un script. Si vous essayez d'ajouter cette valeur à la liste de sécurité globale, un message d'erreur s'affiche en raison de la fonctionnalité de l'agent.
    - `FE9B64DEFD8BF214C7490BB7F35B495A79A95E81F8943EE279DC99998D3D3440`
- Ajouter un certificat à la liste sécurisée globale de CylancePROTECT Desktop
  - Cette méthode nécessite que vous soumettiez un certificat de signature de code valide à la console et est uniquement disponible pour les scripts PowerShell et les scripts actifs (et non les macros).

## Contrôle du terminal

Le contrôle du terminal protège les terminaux en contrôlant les périphériques à mémoire de masse USB connectés aux terminaux de l'organisation. Lorsque vous activez le contrôle des terminaux, vous pouvez autoriser un accès complet, en lecture seule ou bloquer les terminaux de stockage de masse USB, tels que les clés USB, les disques durs externes et les smartphones. Dans le cadre de la stratégie, vous pouvez également utiliser des exclusions pour définir le niveau d'accès pour des terminaux de stockage de masse spécifiques à l'aide de l'ID fournisseur, de l'ID produit et du numéro de série. Par exemple, vous pouvez bloquer tous les terminaux de stockage de masse USB, mais créer des exclusions pour autoriser l'accès complet à certains terminaux autorisés uniquement.

- Le contrôle du terminal est disponible pour les terminaux Windows macOS exécutant l'agent version 2.1.1410 ou ultérieure, et les terminaux exécutant l'agent version 3.3.1000 ou ultérieure.
- Le contrôle du terminal n'affecte pas les terminaux USB tels qu'une souris ou un clavier. Par exemple, lorsque vous créez une stratégie pour bloquer tous les types de terminaux de stockage de masse USB, un utilisateur peut toujours utiliser un clavier USB.

- Le contrôle du terminal n'est pas pris en charge pour les cartes SD pour le moment. Cependant, si elle est utilisée avec un lecteur de carte USB, le contrôle du terminal peut détecter le terminal USB.

Lorsque le contrôle de terminal est activé, tous les terminaux de stockage de masse USB qui sont insérés sont enregistrés, ainsi que l'action de la politique qui a été appliquée (accès complet, lecture seule ou blocage). Si l'action de stratégie est définie sur lecture seule ou blocage et que les notifications de bureau sont activées sur le terminal, une notification contextuelle s'affiche sur le terminal lorsqu'un terminal de stockage de masse USB est connecté. Vous trouverez le journal des évènements de contrôle de terminal sur l'écran **Protection > Terminaux externes** de la console.

| Configuration du contrôle du terminal | Description |
|---|---|
| **Contrôle des terminaux Windows** | Ce paramètre active le contrôle des terminaux Windows et vous permet de sélectionner la stratégie à appliquer pour chaque type de terminal USB.<br>La liste d'exclusion est partagée entre les terminaux Windows et les terminaux macOS lorsque le contrôle des terminaux est activé pour les deux plateformes de système d'exploitation. |
| **Contrôle du terminal macOS** | Ce paramètre active le contrôle des terminaux macOS et vous permet de sélectionner la stratégie à appliquer pour chaque type de terminal USB.<br>La liste d'exclusion est partagée entre les terminaux Windows et les terminaux macOS lorsque le contrôle des terminaux est activé pour les deux plateformes de système d'exploitation. |

| Action de stratégie de contrôle de terminal | Description |
|---|---|
| **Bloquer** | Ce paramètre empêche l'appareil d'accéder aux terminaux de stockage USB externes. |
| **Lecture seule** | Ce paramètre permet un accès en lecture seule aux terminaux de stockage USB externes. L'accès en lecture seule permet aux terminaux d'afficher le contenu d'un terminal USB externe, mais n'autorise pas l'accès en écriture ou en suppression au terminal USB.<br>Les types de terminaux USB suivants peuvent être configurés pour un accès en lecture seule uniquement pour les terminaux Windows :<br>• Image fixe<br>• CD USB / DVD RW<br>• Clé USB<br>• Relais USB VMware<br>• Périphérique portable Windows<br>Lors de l'ajout d'exclusions, ce paramètre s'applique aux terminaux Windows et sera ignoré pour les terminaux macOS. |
| **Accès complet** | Ce paramètre permet l'accès en lecture, écriture et suppression aux terminaux de stockage USB externes. |

| Types de terminaux USB pris en charge | Description | Plateforme d'agent |
|---|---|---|
| **Android** | Il s'agit d'un terminal portable exécutant le système d'exploitation Android, comme un smartphone ou une tablette.<br>Lorsqu'un terminal Android est connecté, il peut être identifié comme terminal Android, d'image fixe ou Windows portable. Si vous souhaitez bloquer les terminaux Android, envisagez également de bloquer les images fixes et les périphériques portables Windows. | Windows |
| **iOS** | Il s'agit d'un terminal portable Apple exécutant iOS, comme un iPhone ou un iPad.<br>Certains terminaux iOS ne se rechargeront pas lorsque le contrôle du terminal est activé et configuré pour bloquer, sauf si le terminal est hors tension. Apple inclut leur capacité de charge dans les fonctions du terminal qui sont nécessaires pour notre capacité de blocage du terminal iOS. Les terminaux autres que Apple ne regroupent pas leur capacité de charge de cette manière et ne sont pas affectés. | Windows |
| **Image fixe** | Ce type de terminaux comprend les scanners, les appareils photo numériques, les caméras vidéo multimodes avec capture d'images et les numériseurs d'images.<br>**Remarque :** L'agent considère les appareils photo Canon comme des terminaux Windows portables, et non comme des terminaux d'image fixes. | Windows |
| **CD USB DVD RW** | Il s'agit d'un lecteur optique USB. | Windows, macOS |
| **Clé USB** | Il s'agit d'un disque dur USB ou d'une clé USB. | Windows, macOS |
| **Relais USB VMware** | C'est un client de machine virtuelle VMware qui dispose de terminaux USB connectés à l'hôte. | Windows |
| **Périphérique portable Windows** | Ce sont des terminaux portables qui utilisent la technologie de pilote Microsoft Windows Portable Device (WPD), tels que les téléphones mobiles, les appareils photo numériques et les lecteurs multimédia portables. | Windows |

#### Ajouter une exclusion de stockage externe

Vous pouvez ajouter des exclusions pour les terminaux de stockage de masse USB externes lorsque vous souhaitez spécifier les autorisations d'accès pour des terminaux de stockage spécifiques. Lorsque vous ajoutez des exclusions à la stratégie de contrôle de terminal, vous avez besoin de l'ID du fournisseur du terminal. L'ID du produit et le numéro de série sont facultatifs et peuvent également être utilisés si vous souhaitez rendre

l'exclusion plus spécifique. Pour vous assurer que vous utilisez les informations correctes pour chaque exclusion, vous pouvez activer le contrôle du terminal, puis insérer un terminal et rechercher son entrée de journal dans la console (**Protection > Terminaux externes**).

Tenez compte des points suivants lorsque vous ajoutez des exclusions de stockage externe :

- Tous les fabricants n'utilisent pas de numéro de série avec leurs produits. Certains fabricants utilisent le même numéro de série pour plusieurs produits.
- Les exclusions de stockage externe ne sont pas modifiables. Ajoutez de nouvelles exclusions si nécessaire et supprimez toutes les exclusions qui ne sont plus nécessaires.
- Il existe une limite de 5 000 exclusions pour chaque stratégie de contrôle de terminal. Le bouton **Ajouter un terminal** est désactivé lorsque cette limite est atteinte.
- La liste d'exclusion est partagée entre les terminaux Windows et les terminaux macOS lorsque le contrôle des terminaux est activé pour les deux plateformes de système d'exploitation.

1. Dans la console, accédez à **Paramètres > Stratégie de terminal**.
2. Créez une stratégie nouvelle ou modifiez-en une existante.
3. Cliquez sur l'onglet **Contrôle du terminal** et assurez-vous que l'option Contrôle du terminal est activée et configurée.
4. Dans la section **Liste d'exclusion de stockage externe**, cliquez sur **Ajouter un terminal**.
5. Saisissez l'**ID du fournisseur**.
6. Vous pouvez inclure l'**ID produit** et le **Numéro de série** pour affiner l'exclusion (facultatif). Vous pouvez également ajouter un commentaire pour décrire l'exclusion.
7. Dans le champ **Accès**, sélectionnez le niveau d'accès que vous souhaitez attribuer :
   - **Accès complet**
   - **Lecture seule**

     Ce paramètre s'applique aux terminaux Windows et sera ignoré pour les terminaux macOS.
   - **Bloquer**
8. Cliquez sur **Envoyer**.
9. Enregistrez (ou créez) la stratégie.

#### Importation en bloc d'exclusions de contrôle du terminal

Les administrateurs peuvent utiliser un fichier .csv pour importer en masse des exclusions de contrôle des terminaux (jusqu'à 500 exclusions par fichier). Pour plus d'informations sur les exigences de formatage et pour télécharger un modèle, rendez-vous sur support.blackberry.com pour lire l'article de la base de connaissances 65484.

#### Télécharger le modèle .csv d'exclusion de contrôle de terminal

1. Dans l'onglet **Contrôle du terminal** de la stratégie de terminal, activez Contrôle du terminal.
2. Cliquez sur **Importer les exclusions**.
3. Cliquez sur **Télécharger notre modèle** et enregistrez le fichier.
4. Modifiez le modèle en fonction des exigences de formatage.

#### Importer un fichier .csv avec les exclusions de contrôle de terminal

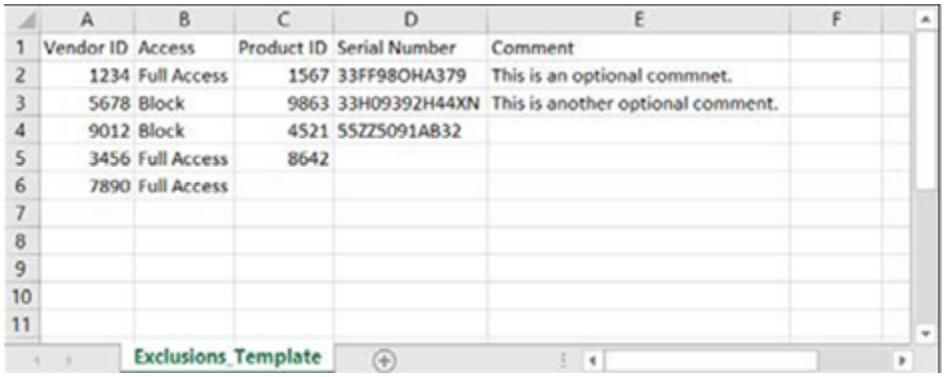
1. Dans l'onglet **Contrôle du terminal** de la stratégie de terminal, activez Contrôle du terminal.
2. Cliquez sur **Importer les exclusions**.
3. Cliquez sur **Rechercher les fichiers CSV à importer** et sélectionnez le fichier .csv à importer.

4. Cliquez sur **Télécharger**.

#### Exigences de formatage du fichier .csv

- Seuls les fichiers .csv sont acceptés.
- Les informations d'entête de la colonne sont requises dans le fichier .csv. La fonction d'importation ignore la première ligne du fichier .csv. Si la première ligne du fichier d'importation est une exclusion, elle ne sera pas importée. Les entêtes de colonne doivent être dans l'ordre suivant :
  - ID du fournisseur
  - Accès
  - ID du produit
  - Numéro de série
  - Commentaire
- L'identifiant du fournisseur et les champs d'accès sont requis pour chaque exclusion.
- Les champs ID produit, Numéro de série et Commentaire sont facultatifs pour chaque exclusion.
- La colonne Accès requiert comme valeur soit `Accès complet`, soit `Lecture seule`, soit `Bloquer` et n'accepte que les valeurs en anglais.
- La colonne Commentaires ne prend pas en charge les virgules (,).

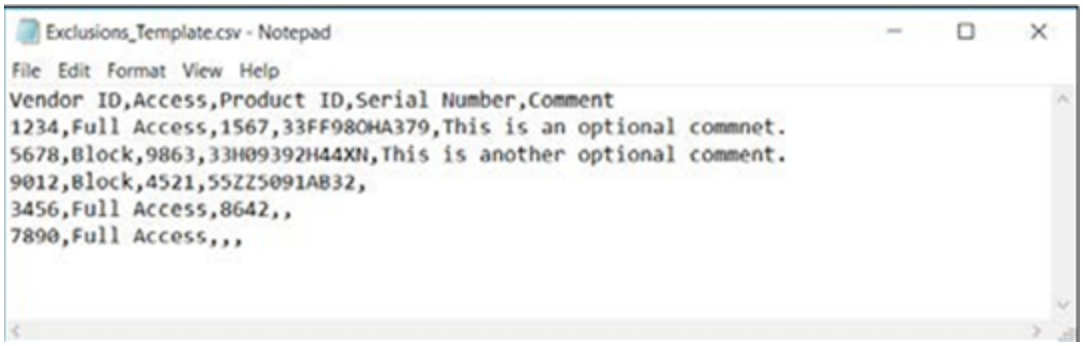
**Exemple :** importation en bloc à l'aide d'une feuille de calcul



| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 1 | Vendor ID | Access | Product ID | Serial Number | Comment | |
| 2 | 1234 | Full Access | 1567 | 33FF98OHA379 | This is an optional commnet. | |
| 3 | 5678 | Block | 9863 | 33H09392H44XN | This is another optional comment. | |
| 4 | 9012 | Block | 4521 | 55ZZ5091AB32 | | |
| 5 | 3456 | Full Access | 8642 | | | |
| 6 | 7890 | Full Access | | | | |
| 7 | | | | | | |
| 8 | | | | | | |
| 9 | | | | | | |
| 10 | | | | | | |
| 11 | | | | | | |

Exclusions_Template

**Exemple :** importation en bloc à l'aide d'un éditeur de texte



Exclusions_Template.csv - Notepad

File Edit Format View Help

```
Vendor ID,Access,Product ID,Serial Number,Comment
1234,Full Access,1567,33FF98OHA379,This is an optional commnet.
5678,Block,9863,33H09392H44XN,This is another optional comment.
9012,Block,4521,55ZZ5091AB32,
3456,Full Access,8642,,
7890,Full Access,,,
```

#### Limites

- Le nombre maximal d'exclusions par fichier .csv est de 500. Si vous essayez d'importer un fichier contenant plus de 500 exclusions, un message d'erreur s'affiche.

- Le nombre maximal d'exclusions de contrôle des terminaux par stratégie est de 5 000. Un message d'avertissement doit s'afficher si ce nombre est dépassé.
- Si vous utilisez un terminal dont la langue n'est pas l'anglais, vous devrez peut-être définir les options sur UTF-8 et séparées par des virgules lorsque vous importez et modifiez le modèle avec Microsoft Excel. Si vous ouvrez le fichier sans modifier les options, il peut afficher des caractères non reconnaissables.

# Installation de l'agent CylancePROTECT Desktop pour Windows

CylancePROTECT Desktop détecte et bloque les programmes malveillants avant qu'ils n'affectent un terminal. BlackBerry utilise une approche mathématique de l'identification des programmes malveillants, à l'aide de techniques d'apprentissage automatique au lieu de signatures réactives, de systèmes basés sur la confiance ou de bacs à sable. Cette approche neutralise les nouveaux programmes malveillants, virus, bots et variantes futures. CylancePROTECT Desktop analyse les exécutions potentielles de fichiers à la recherche de programmes malveillants dans les couches de système d'exploitation et de mémoire afin d'empêcher la distribution de charges utiles malveillantes.

Vous pouvez installer l'agent sur des terminaux spécifiques ou utiliser les paramètres d'installation pour le déployer dans votre environnement à l'aide d'un outil de déploiement.

## Installer l'agent Windows

**Avant de commencer :**

- Téléchargez les fichiers d'installation à CylancePROTECT Desktop partir de la console de gestion. Cliquez sur **Paramètres > Déploiements**. Dans la liste déroulante **Produit**, sélectionnez **CylancePROTECT**, et définissez le système d'exploitation cible, la version de l'agent et le type de fichier. Cliquez sur **Télécharger**.
- Dans la console de gestion, copiez le jeton d'installation depuis **Paramètres > Application**.

1. Double-cliquez sur le programme d'installation CylancePROTECT Desktop.
2. Dans la fenêtre de configuration de CylancePROTECT Desktop, cliquez sur **Installer**.
3. Saisissez le jeton d'installation et cliquez sur **Suivant**.
4. Vous pouvez également modifier le dossier de destination.
5. Cliquez sur **OK** pour lancer l'installation.
6. Cliquez sur **Terminer** pour terminer l'installation. Assurez-vous que la case à cocher pour le lancement de CylancePROTECT Desktop est sélectionnée.

**À la fin :** Si la protection de la mémoire, le contrôle des scripts et/ou le contrôle du terminal sont activés dans la stratégie de terminal, un redémarrage du terminal après l'installation ou la mise à niveau de l'agent est recommandé, mais pas strictement requis. Un redémarrage permet de s'assurer que tous les nouveaux paramètres de stratégie sont pleinement pris en compte.

## Paramètres d'installation Windows

L'agent peut être installé de manière interactive ou non interactive via GPO, Microsoft System Center Configuration Manager (SCCM), MSIEXEC et d'autres outils tiers. Les MSI peuvent être personnalisés avec les paramètres ci-dessous ou les paramètres peuvent être fournis à partir de la ligne de commande.

| Paramètre | Valeur | Description |
|---|---|---|
| PIDKEY | *<Installation Token>* | Ce paramètre saisit automatiquement le jeton d'installation. |

| Paramètre | Valeur | Description |
| --- | --- | --- |
| LAUNCHAPP | 0 ou 1 | 0 : cette valeur masque l'icône de la barre d'état système dans le dossier du menu Démarrer au moment de l'exécution.<br>1 : cette valeur affiche l'icône de la barre d'état système dans le dossier du menu Démarrer au moment de l'exécution.<br>Si aucune valeur n'est saisie, la valeur par défaut est 1. |
| SELFPROTECTIONLEVEL | 1 ou 2 | 1 : cette valeur permet aux administrateurs locaux d'apporter des modifications au registre et aux services.<br>2 : cette valeur permet uniquement à l'administrateur système d'apporter des modifications au registre et aux services.<br>Si aucune valeur n'est saisie, la valeur par défaut est 2. |
| APPFOLDER | *<Target Installation Folder>* | Ce paramètre spécifie le répertoire d'installation de l'agent. L'emplacement par défaut est C:\Program Files\Cylance\Desktop |

| Paramètre | Valeur | Description |
|---|---|---|
| REGWSC | 0 ou 1 | 0 : cette valeur indique que CylancePROTECT Desktop n'est pas enregistré sous Windows en tant que programme antivirus. Cela permet à CylancePROTECT Desktop et à Windows Defender de s'exécuter en même temps sur le terminal.<br><br>1 : cette valeur indique que CylancePROTECT Desktop est enregistré sous Windows en tant que programme antivirus.<br><br>Si aucune valeur n'est saisie, la valeur par défaut est 1.<br><br>Les commandes ci-dessus n'auront aucun effet sur Windows Server 2016 et 2019. Pour désactiver Windows Defender après l'installation de CylancePROTECT Desktop sur Windows Server 2016 et 2019, définissez la valeur de registre suivante :<br><br>`HKLM\SOFTWARE\Policies\Microsoft \Windows Defender\DisableAntiSpyware`<br><br>`REG_DWORD`<br><br>`Value = 1`<br><br>Si la sous-clé Windows Defender n'existe pas, vous devrez la créer manuellement.<br><br>Pour plus d'informations sur l'utilisation des paramètres de la stratégie de groupe pour gérer Windows Defender, consultez Utiliser les paramètres de stratégie de groupe pour configurer et gérer Windows Defender AV. |
| VENUEZONE | « *<Zone_Name>* » | Utilisez ce paramètre pour indiquer le nom d'une zone à laquelle vous souhaitez ajouter des services. S'il ne trouve pas de zone portant ce nom, il crée une zone portant le nom que vous avez indiqué.<br><br>Les noms de zone ne peuvent pas contenir d'espaces, de tabulations, de retours chariot, de signes égal, de nouvelles lignes, ou d'autres caractères invisibles. |

| Paramètre | Valeur | Description |
|---|---|---|
| VDI | <X> | Lorsque vous installez CylancePROTECT Desktop sur une image maître, utilisez le paramètre d'installation VDI=<*X*> où <*X*> est un « compteur » pour le nombre total de machines ou d'images non connectées au domaine (y compris l'image maître) avant de créer un pool de postes de travail. La valeur de <*X*> détermine quand l'agent doit commencer à identifier la machine virtuelle à l'aide de l'empreinte VDI au lieu du mécanisme d'empreinte par défaut de l'agent.<br><br>Le paramètre VDI utilise un compteur X et a un effet différé, alors que le paramètre AD est immédiat lors de l'installation.<br><br>Pour plus d'informations, consultez Configuration requise et considérations relatives à l'utilisation de CylancePROTECT Desktop sur des machines virtuelles. |
| AD | 1 | Ce paramètre nécessite la version 1520 ou ultérieure de l'agent.<br><br>Utilisez le paramètre Active Directory (AD) sur une image principale connectée au domaine lors de l'installation initiale. Lorsqu'il est installé sur une image maître connectée à un domaine, il utilise immédiatement l'empreinte VDI sur l'image maître et crée ensuite un pool de postes de travail.<br><br>L'empreinte AD prévaut sur le paramètre d'installation VDI=<*X*>. Pour plus d'informations, consultez Configuration requise et considérations relatives à l'utilisation de CylancePROTECT Desktop sur des machines virtuelles. |
| PROXY_SERVER | <*ip_address*>:<br><*port_ number*> | Ce paramètre spécifie l'adresse IP du serveur proxy via lequel l'agent doit communiquer. Les paramètres du serveur proxy sont ajoutés au registre du terminal et vous pouvez trouver des informations sur le serveur proxy dans le fichier journal de l'agent. |

| Paramètre | Valeur | Description |
|---|---|---|
| AWS | 1 | Ce paramètre nécessite la version 1500 ou ultérieure de l'agent.<br><br>Utilisez ce paramètre pour capturer et inclure l'ID d'instance Amazon EC2 au nom du terminal afin de faciliter l'identification des hôtes cloud Amazon.<br><br>Le nom du terminal est modifié pour inclure le nom d'hôte et l'ID d'instance. Par exemple, si le nom du terminal est ABC-DE-12345678 et que l'ID AWS EC2 est i-0a1b2cd34efg56789, le nom complet du terminal est ABC-DE-123456789_i-0a1b2cd34efg56789.<br><br>Cette fonctionnalité est uniquement disponible pour l'ID d'instance Amazon EC2. |
| PROTECTTEMPPATH | 1 | Ce paramètre nécessite la version 1480 ou une version ultérieure de l'agent.<br><br>Utilisez ce paramètre pour modifier l'emplacement des dossiers CylanceDesktopArchive et CylanceDesktopRemoteFile vers le dossier Cylance ProgramData.<br><br>Pour plus d'informations, consultez l'article KB 66457 Modifier l'emplacement des dossiers CylanceDesktopArchive et CylanceDesktopRemoteFile. |

**Exemple : paramètres PIDKEY, APPFOLDER et LAUNCHAPP**

```
msiexec /i CylancePROTECT_x64.msi /qn PIDKEY=<INSTALLATION TOKEN> LAUNCHAPP=0 /L*v
 C:\temp\install.log
```

Dans cet exemple, l'installation est silencieuse et le journal d'installation est enregistré dans le dossier `C:\temp`. Vous devrez peut-être créer ce dossier. Lorsque l'agent est en cours d'exécution, l'icone de la barre d'état système et le dossier Cylance du menu Démarrer sont masqués. Pour plus d'informations sur les options de ligne de commande autorisées, consultez https://docs.microsoft.com/en-us/windows/win32/msi/command-line-options.

**Exemple : paramètres PIDKEY, VDI et LAUNCHAPP**

```
msiexec /i CylancePROTECT_x64.msi /qn PIDKEY=<INSTALLATION TOKEN> VDI=2
 LAUNCHAPP=1
```

Dans cet exemple, « 2 » pour VDI correspond au nombre total de machines ou d'images qui ne sont pas connectées au domaine (l'image principale plus l'image supplémentaire ou l'image parente) avant la création du pool de postes de travail.

**Exemple : paramètres PIDKEY, AD et LAUNCHAPP**

```
msiexec /i CylancePROTECT_x64.msi /qn PIDKEY=<INSTALLATION TOKEN> AD=1 LAUNCHAPP=1
```

Dans cet exemple, le paramètre AD utilise immédiatement l'empreinte VDI sur l'image principale et le pool de postes de travail créés. Pour obtenir des informations sur la modification du fichier d'installation MSI pour le déploiement via la stratégie de groupe, consultez l'article KB 66391 Modifier le programme d'installation MSI à l'aide d'Orca.

# Installation de l'agent CylancePROTECT Desktop pour macOS

CylancePROTECT Desktop détecte et bloque les programmes malveillants avant qu'ils n'affectent un terminal. BlackBerry utilise une approche mathématique de l'identification des programmes malveillants, à l'aide de techniques d'apprentissage automatique au lieu de signatures réactives, de systèmes basés sur la confiance ou de bacs à sable. Cette approche neutralise les nouveaux programmes malveillants, virus, bots et variantes futures. CylancePROTECT Desktop analyse les exécutions potentielles de fichiers à la recherche de programmes malveillants dans les couches de système d'exploitation et de mémoire afin d'empêcher la distribution de charges utiles malveillantes.

Vous pouvez installer l'agent sur des terminaux spécifiques ou utiliser les paramètres d'installation pour le déployer dans votre environnement à l'aide d'un outil de déploiement.

## Installer l'agent CylancePROTECT Desktop sur macOS

**Avant de commencer :**

- Téléchargez les fichiers d'installation à CylancePROTECT Desktop partir de la console de gestion. Cliquez sur **Paramètres > Déploiements**. Dans la liste déroulante **Produit**, sélectionnez **CylancePROTECT**, et définissez le système d'exploitation cible, la version de l'agent et le type de fichier. Cliquez sur **Télécharger**.
- Dans la console de gestion, copiez le jeton d'installation depuis **Paramètres > Application**.

1. Double-cliquez sur le fichier d'installation CylancePROTECT Desktop (.dmg ou .pkg) pour monter le programme d'installation.
2. Double-cliquez sur  dans l'interface utilisateur CylancePROTECT Desktop pour lancer l'installation.
3. Cliquez sur **Continuer** pour vérifier que le système d'exploitation et le matériel répondent à la configuration requise.
4. Cliquez sur **Continuer**.
5. Saisissez le jeton d'installation.
6. Cliquez sur **Continuer**.
7. Vous pouvez également modifier l'emplacement d'installation.
8. Cliquez sur **Installer**.
9. Saisissez vos informations d'identification.
10. Cliquez sur **Installer le logiciel**.
11. Dans l'écran récapitulatif, cliquez sur **Fermer**.
12. Cliquez sur **OK > Terminer**.
13. Si vous effectuez l'installation de CylancePROTECT Desktop sous macOS Catalina, une notification vous invite à autoriser CylanceUI à afficher les notifications. Cliquez sur **Allow** (Autoriser).

#### Configuration requise de CylancePROTECT Desktop pour macOS et versions ultérieures

Pour installer l'agent CylancePROTECT Desktop version 2.1 ou versions ultérieures sur les terminaux dotés de macOS, notez les exigences de configuration suivantes. Les exigences varient selon que les terminaux sont gérés par une solution MDM (par exemple, Jamf Pro).

#### Terminaux gérés par MDM

Les informations ci-dessous utilisent Jamf Pro comme solution MDM, mais elles s'appliquent à d'autres solutions MDM.

| Configuration requise | Étapes |
|---|---|
| Paramètres généraux | Créez un profil de configuration et spécifiez les paramètres suivants dans l'onglet Général :<br>• Saisissez le nom et la description du profil.<br>• Niveau : niveau de l'ordinateur<br>• Méthode de distribution : installation automatique |
| Activez l'extension kernel de CylancePROTECT. (macOS 10 uniquement) | Configurez les paramètres suivants à partir de l'option Extensions de Kernel approuvées :<br>• Nom affiché : Cylance<br>• Identifiant de l'équipe : 6ENJ69K633<br>• Dans l'onglet **Étendue**, vérifiez que le profil de configuration est défini pour s'appliquer aux terminaux qui exécutent macOS 10 CylancePROTECT Desktop et CylanceOPTICS. |
| Activez l'extension système CylancePROTECT. (macOS 11+) | Configurez les paramètres suivants à partir de l'option Extensions système :<br>• Nom d'affichage : CylanceSystemExtension<br>• Types d'extension système : extensions système autorisées<br>• Identifiant de l'équipe : 6ENJ69K633<br>• Extensions système autorisées : com.cylance.CylanceEndpointSecurity.extension |

| Configuration requise | Étapes |
| --- | --- |
| Activez l'accès complet au disque pour l'agent CylancePROTECT et les extensions système. | Configurez les paramètres suivants à partir de l'option Préférences de confidentialité et Contrôle de la stratégie.<br>Ajoutez une configuration d'accès aux applications et spécifiez les paramètres suivants :<br>• Identifiant : com.cylance.Agent<br>• Type d'identifiant : ID de lot<br>• Exigence de code :<br>Copiez l'exigence de code de la version HTML de cette rubrique. L'exigence de code doit se trouver sur une ligne et ne doit pas comporter d'espaces ni de sauts de ligne supplémentaires.<br>• Ajoutez le service **SystemPolicyAllFiles** et définissez sur **Autoriser**.<br>Ajoutez une autre configuration d'accès aux applications et spécifiez les paramètres suivants :<br>• Identifiant : com.cylance.CylanceEndpointSecurity.extension<br>• Type d'identifiant : ID de lot<br>• Exigence de code :<br>Copiez l'exigence de code de la version HTML de cette rubrique. L'exigence de code doit se trouver sur une ligne et ne doit pas comporter d'espaces ni de sauts de ligne supplémentaires.<br>• Ajoutez le service **SystemPolicyAllFiles** et définissez sur **Autoriser**. |
| Notifications | Dans l'onglet Notifications du profil de configuration, les paramètres suivants sont recommandés :<br>• Alertes critiques : activées<br>• Notifications : activées<br>• Type d'alerte de bannière : persistante<br>• Notifications sur l'écran de verrouillage : s'affichent<br>• Notifications dans le Centre de notifications : s'affichent<br>• Icône de l'application badge : s'affiche<br>• Émettre un son pour les notifications : activé |
| Portée | Configurez les paramètres suivants dans l'onglet Étendue :<br>• Vérifiez que le profil de configuration est défini pour s'appliquer aux terminaux qui exécutent macOS CylancePROTECT Desktop. |
| Redémarrez après l'installation. | Après avoir effectué les étapes de configuration ci-dessus et installé l'agent CylancePROTECT Desktop, redémarrez le terminal. |

#### Terminaux qui ne sont pas gérés par MDM

Sur les terminaux qui ne sont pas gérés par MDM, l'utilisateur reçoit une invite pour approuver l'extension système CylanceES après l'installation de l'agent macOS sur le terminal. Suivez ces instructions à l'invite pour activer l'extension système et autoriser l'accès complet au disque. Les utilisateurs peuvent également appuyer sur la notification dans « CylanceUI » pour configurer ses paramètres de notification.

1. Cliquez sur **Ouvrir les préférences de sécurité**. L'onglet **Préférences système** > **Sécurité et confidentialité** > **Général** s'ouvre.
2. Si nécessaire, cliquez sur le verrou pour authentifier les modifications, puis cliquez sur **Autoriser**.
3. En regard du message **Le logiciel système de l'application « CylanceES » n'a pas pu être chargé**, cliquez sur **Autoriser** pour approuver l'extension.
4. Pour activer l'accès complet au disque, accédez à **Préférences système** > **Sécurité et confidentialité** > **Confidentialité**.
5. Si nécessaire, cliquez sur le verrou pour authentifier les modifications, puis cliquez sur **Autoriser**.
6. Faites défiler vers le bas et cliquez sur **Accès complet au disque**.
7. Sélectionnez **CylanceEsExtension**.
8. Autorisez les notifications pour l'agent à partir de l'onglet **Préférences système** > **Notifications** > **CylanceUI**.

#### Commandes d'installation de l'agent macOS en ligne de commande

Lorsque vous utilisez la ligne de commande pour installer l'agent macOS, vous devez créer un fichier `cyagent_install_token` qui inclut les paramètres d'installation. Le fichier inclut le jeton d'installation, ainsi que d'autres paramètres facultatifs que vous pouvez définir.

Les sections suivantes comprennent des exemples de création du fichier en ligne de commande, mais vous pouvez créer le fichier à partir d'un éditeur de texte qui inclut chaque paramètre dans sa propre ligne distincte. Le fichier doit se trouver dans le même dossier que le package d'installation.

#### Installer l'agent macOS avec jeton d'installation uniquement

Utilisez les exemples de commandes suivants dans le terminal pour créer le fichier `cyagent_ install_token` avec le jeton d'installation et installer l'agent. Si vous utilisez le programme d'installation .dmg, modifiez l'extension de fichier dans la commande en conséquence.

```
echo YOURINSTALLTOKEN > cyagent_install_token
sudo installer -pkg CylancePROTECT.pkg -target /
```

Voici la commande d'installation sans jeton d'installation :

```
sudo installer -pkg CylancePROTECT.pkg -target /
```

#### Installer l'agent macOS avec les paramètres spécifiés

Utilisez les exemples de commandes suivants dans le terminal pour créer le fichier `cyagent_ install_token` avec les paramètres spécifiés et installer l'agent. Si vous utilisez le programme d'installation .dmg, modifiez l'extension de fichier dans la commande en conséquence.

```
echo YOURINSTALLTOKEN > cyagent_install_token
echo SelfProtectionLevel=2 >> cyagent_install_token
echo VenueZone=nom_zone >> cyagent_install_token
echo LogLevel=2 >> cyagent_install_token
sudo installer -pkg CylancePROTECT.pkg -target /
```

#### Paramètres d'installation

L'agent CylancePROTECT Desktop peut être installé à l'aide des options de ligne de commande du terminal.

| Paramètre | Valeur | Description |
|---|---|---|
| `InstallToken` | *<jeton_installation>* | Le jeton d'installation est requis lorsque vous installez l'agent. Vous pouvez le trouver dans la console de gestion en cliquant sur **Paramètres > Application**. |
| `NoCylanceUI` | | Ce paramètre masque la barre d'état système au démarrage. |
| `SelfProtectionLevel` | 1 ou 2 | 1 : cette valeur permet aux administrateurs locaux seulement d'apporter des modifications au registre et aux services.<br>2 : cette valeur permet uniquement à l'administrateur système d'apporter des modifications au registre et aux services.<br>Si aucune valeur n'est spécifiée, la valeur par défaut est 2. |
| `LogLevel` | 0, 1, 2, ou 3 | 0 : cette valeur indique que seuls les messages d'erreur sont enregistrés.<br>1 : cette valeur indique que les messages d'erreur et d'avertissement sont enregistrés.<br>2 : cette valeur indique que les messages d'erreur, d'avertissement et d'information sont enregistrés.<br>3 : cette valeur active la journalisation détaillée, où tous les messages sont consignés. Notez que la taille des fichiers journaux détaillés peut augmenter considérablement. BlackBerry recommande d'activer le niveau détaillé pendant la résolution des problèmes, puis de le rétablir sur 2 une fois la résolution des problèmes terminée.<br>Si aucune valeur n'est spécifiée, la valeur par défaut est 2. |
| `VenueZone` | *<nom_zone>* | Utilisez ce paramètre pour ajouter des périphériques à une zone existante ou à une zone que vous souhaitez créer. Si la zone n'existe pas, elle sera créée à l'aide du nom fourni.<br>Vous ne pouvez pas utiliser d'onglets, de retours chariot, de nouvelles lignes, de signes égaux, d'espaces ou d'autres caractères invisibles dans le nom de la zone.<br>Ce paramètre nécessite la version 1380 ou ultérieure de l'agent. |
| `ProxyServer` | *<adresse_ip>*:*<numéro* | Cela ajoute des paramètres de serveur proxy au registre du terminal. Vous trouverez les informations relatives au serveur proxy dans le fichier journal de l'agent.<br>Ce paramètre nécessite la version 1470 ou ultérieure de l'agent. |

## Résolution des problèmes rencontrés lors de l'installation de macOS

Le tableau ci-dessous décrit les actions que vous pouvez effectuer pour résoudre les problèmes d'installation de macOS.

| Problème | Action |
| --- | --- |
| Dépannage à l'aide du jeton d'installation et de la journalisation détaillée du programme d'installation | Saisissez les commandes suivantes et remplacez « YOURINSTALLTOKEN » par le jeton d'installation qui se trouve dans l'onglet **Paramètres > Application** de la console de gestion :<br>`echo YOURINSTALLTOKEN >cyagent_install_token`<br>`sudo installer -verboseR -dumplog -pkg CylancePROTECT.pkg -target /`<br>La commande echo génère un fichier texte `cyagent_install_token` contenant une option d'installation par ligne. Le fichier doit se trouver dans le même dossier que le package d'installation `CylancePROTECT.pkg`.<br>Si vous installez l'agent CylancePROTECT Desktop à l'aide du terminal sur macOS Catalina, un avertissement DYLD s'affiche parfois. Cet avertissement n'affecte pas l'installation, car il est généré par le système d'exploitation et non par le CylancePROTECT Desktop. |
| Démarrer ou arrêter le service d'agent sous macOS | Pour démarrer le service de l'agent, exécutez la commande suivante :<br>`sudo launchctl load /Library/launchdaemons/com.cylance.agent_service.plist`<br>Pour arrêter le service de l'agent, exécutez la commande suivante :<br>`sudo launchctl load /Library/launchdaemons/com.cylance.agent_service.plist` |

| Problème | Action |
| --- | --- |
| Prise en charge de l'extension de système Endpoint Security sur macOS Big Sur | BlackBerry recommande d'utiliser MDM pour déployer un profil de configuration qui contient l'approbation et l'accès au disque complet pour l'extension du système CylancePROTECT Desktop. Par défaut, macOS Big Sur ne prend pas en charge les installations silencieuses à distance d'un profil MDM sur un système avec une nouvelle installation du système d'exploitation Big Sur.<br><br>Pour installer des profils de configuration sur des systèmes macOS distants, sans intervention de l'utilisateur (installation silencieuse), Mobile Device Management (Gestion des terminaux mobiles) d'Apple est requis. Avant la mise à niveau vers macOS Big Sur, les terminaux doivent être inscrits auprès d'un fournisseur MDM. Les terminaux non inscrits avant la mise à niveau requièrent l'intervention d'un utilisateur avec des privilèges d'administration.<br><br>Pour prendre en charge les installations silencieuses à distance, procédez comme suit :<br><br>**1.** Installez macOS Catalina.<br>**2.** Appliquez le profil MDM.<br>**3.** Téléchargez les profils de configuration sur le terminal.<br>**4.** Mettez à niveau le terminal vers macOS Big Sur.<br><br>Les versions d'agent CylancePROTECT Desktop et les types d'extension pris en charge sont les suivants :<br><br>• Les versions 1570 ou antérieures de l'agent CylancePROTECT Desktop incluent l'extension du noyau qui est prise en charge sur macOS Catalina ou une version antérieure.<br>• Les versions 1580 et ultérieures de l'agent CylancePROTECT Desktop incluent l'extension de noyau prise en charge par macOS Catalina ou une version antérieure, ainsi que l'extension de système Endpoint Security, prise en charge par macOS Big Sur et les versions ultérieures. |

# Installation de l'agent CylancePROTECT Desktop pour Linux

L'agent peut être installé directement sur chaque système ou via un logiciel de gestion du système, tel qu'Ansible, SCCM ou cloud-init. Lors de l'installation de l'agent, des paramètres d'installation sont fournis pour configurer certains paramètres d'installation.

Assurez-vous que les terminaux cibles répondent à la configuration système requise et que vous disposez des autorisations appropriées pour installer le logiciel.

- Consultez la configuration requise pour CylancePROTECT Desktop.
- Une autorisation racine est requise pour installer l'agent Linux.
- Créer un fichier de configuration pour l'installation de l'agent Linux

Après avoir installé l'agent CylancePROTECT Desktop sur les terminaux Linux, veillez à maintenir les pilotes Linux à jour de façon à ce qu'ils prennent en charge les derniers noyaux sur les systèmes. Des packages de pilotes mis à jour sont publiés régulièrement, quelles que soient les versions de l'agent. Pour plus d'informations, consultez Mettre à niveau le pilote Linux.

#### Package d'installation de l'agent Linux

À partir de la version 2.1.1590 de l'agent, les packages de pilotes, l'interface utilisateur de l'agent et l'agent CylancePROTECT Desktop sont inclus dans un fichier compressé .tgz.

| Package Debian | Composant |
|---|---|
| cylance-protect-driver | Pilote propriétaire |
| cylance-protect-open-driver | Pilote d'ouverture |
| cylance-protect | Agent/service CylancePROTECT Desktop |
| cylance-protect-ui | Interface utilisateur CylancePROTECT Desktop |

| Package RPM | Composant |
|---|---|
| CylancePROTECTDriver | Pilote propriétaire |
| CylancePROTECTOpenDriver | Pilote d'ouverture |
| CylancePROTECT | Agent/service CylancePROTECT Desktop |
| CylancePROTECTUI | Interface utilisateur CylancePROTECT Desktop |

## Conditions préalables à l'installation sous Linux

L'agent peut être installé directement sur chaque système ou via un logiciel de gestion du système, tel qu'Ansible, SCCM ou cloud-init. Lors de l'installation de l'agent, des paramètres d'installation sont fournis pour configurer certains paramètres d'installation.

Assurez-vous que les terminaux cibles répondent à la configuration système requise et que vous disposez des informations d'identification appropriées pour installer le logiciel.

- Configuration requise pour CylancePROTECT Desktop
- Une autorisation racine est requise pour installer l'agent Linux.

#### Créer un fichier de configuration pour l'installation de l'agent Linux

Avant d'installer l'agent CylancePROTECT Desktop sur les terminaux Linux, vous devez créer un fichier de configuration servant à enregistrer le terminal auprès de votre locataire Cylance Endpoint Security et à définir les paramètres de l'agent local. Au terme de l'installation de l'agent, le fichier de configuration est supprimé du terminal.

CylancePROTECT Desktop requiert que le fichier `config_defaults.txt` contienne uniquement un saut de ligne comme fin de ligne. Si vous créez le fichier à partir d'un ordinateur DOS/Windows, la fin de ligne inclut le retour charriot et le saut de ligne. Pour obtenir des instructions sur la conversion du fichier config_defaults.txt en un format approprié, rendez-vous sur support.blackberry.com/community pour consulter l'article 65749.

1. Dans le répertoire `/opt/cylance/`, créez le fichier `config_defaults.txt`.
2. Modifiez le fichier avec les informations suivantes.

```
InstallToken=YOUR_INSTALL_TOKEN
SelfProtectionLevel=2
```

```
LogLevel=2
VenueZone=ZONE_NAME
UiMode=2
AWS=1
```

- Remplacez *YOUR_INSTALL_TOKEN* par le jeton d'installation de la console de gestion.
- Remplacez *ZONE_NAME* par le nom de la zone où vous souhaitez ajouter le terminal. Si la zone spécifiée n'existe pas dans la console, elle est automatiquement créée.

| Paramètre | Description |
|---|---|
| **InstallToken** | Ce champ est obligatoire et spécifie le locataire Cylance Endpoint Security avec lequel vous souhaitez enregistrer le terminal. Utilisez le jeton d'installation du menu **Paramètres > Application** de la console de gestion. |
| **SelfProtectionLevel** | Ce paramètre limite le niveau d'accès au service Cylance et aux dossiers.<br>• `1` : seuls les administrateurs locaux peuvent apporter des modifications au registre et aux services.<br>• `2` : seul l'administrateur système peut apporter des modifications au registre et aux services.<br>Le paramètre par défaut est « 2 ». |
| **LogLevel** | Ce paramètre spécifie le niveau des informations collectées dans les journaux de débogage.<br>• `0` : Erreur<br>• `1` : Avertissement<br>• `2` : Information<br>• `3` : Détaillé<br>Le paramètre par défaut est « 2 ». Si la journalisation détaillée est sélectionnée, la taille du fichier journal augmente rapidement. |
| **VenueZone** | Ce paramètre spécifie la zone à laquelle vous souhaitez ajouter le terminal.<br>• Si le nom de la zone spécifiée n'existe pas dans la console, la zone est créée à l'aide du nom fourni.<br>• Si le nom de la zone ou du terminal commence ou se termine par un espace (par exemple, «  Hello » ou « Hello  »), il est supprimé lors de l'enregistrement du terminal. Les onglets, les retours chariot, les nouvelles lignes ou tout autre caractère invisible ne sont pas autorisés.<br>• Les noms de zone ne peuvent pas contenir le signe égal (=). Par exemple, « Hello=World » n'est pas autorisé. |
| **UiMode** | Ce paramètre spécifie le mode d'interface utilisateur de l'agent au démarrage du système.<br>• `1` : interface utilisateur minimale<br>• `2` : interface utilisateur complète<br>Le paramètre par défaut est « 2 ». |

| Paramètre | Description |
| --- | --- |
| **AWS** | Ce paramètre indique que l'agent s'exécute sur un hôte Amazon Web Services. Par défaut, le nom d'hôte du terminal est utilisé comme nom de terminal dans la console de gestion. Activez ce paramètre pour permettre à l'agent de capturer l'ID d'instance de l'hôte et de le stocker avec le nom d'hôte dans le champ Nom du terminal de la console. Ce paramètre garantit que chaque agent d'un hôte Amazon Web Services signale un nom de terminal unique à la console de gestion.<br>`1` : permet à l'agent de capturer l'ID d'instance.<br>Le nom du terminal est modifié pour inclure le nom d'hôte + l'ID d'instance. L'ID d'instance est indiqué par le préfixe « i- ».<br>ABC-DE-123456789_i-0a1b2cd34efg56789, où le nom du terminal est ABCDE- 12345678 et l'ID AWS EC2 est i-0a1b2cd34efg56789. |

## Installer l'agent Linux automatiquement

**Avant de commencer :**

- Consultez la configuration requise pour CylancePROTECT Desktop.
- Téléchargez les fichiers d'installation à CylancePROTECT Desktop partir de la console de gestion. Cliquez sur **Paramètres > Déploiements**. Dans la liste déroulante **Produit**, sélectionnez **CylancePROTECT**, et définissez le système d'exploitation cible, la version de l'agent et le type de fichier. Cliquez sur **Télécharger**.
- Dans la console de gestion, copiez le jeton d'installation depuis **Paramètres > Application**.
- Vérifiez que vous disposez des autorisations root.

1. Créer un fichier de configuration pour l'installation de l'agent Linux.
2. Utilisez les commandes suivantes dans l'ordre indiqué pour installer le pilote et l'agent. Utilisez les fichiers extraits du fichier .tgz pour déterminer la valeur de *<version>*.

| Distribution Linux | Commandes |
| --- | --- |
| • Red Hat Enterprise Linux<br>• CentOS<br>• Amazon Linux<br>• Oracle | Utilisez les commandes suivantes pour installer le pilote et l'agent :<br>**a.** `yum install CylancePROTECTOpenDriver-<version>.rpm CylancePROTECTDriver-<version>.rpm`<br>**b.** `yum install CylancePROTECT.<version>.rpm CylancePROTECTUI.<version>.rpm` |
| SUSE Linux Enterprise Server | Utilisez les commandes suivantes pour installer le pilote et l'agent :<br>**a.** `zypper install CylancePROTECTOpenDriver-<version>.rpm CylancePROTECTDriver-<version>.rpm`<br>**b.** `zypper install CylancePROTECT.<version>.rpm CylancePROTECTUI.<version>.rpm` |

**À la fin :**

- Si l'interface utilisateur de l'agent ne démarre pas automatiquement après l'installation (par exemple, sur les terminaux CentOS, SUSE ou Ubuntu), vous devez redémarrer GNOME Shell pour afficher l'interface utilisateur CylancePROTECT. Reportez-vous à la section Démarrer l'interface utilisateur manuellement.

## Installer l'agent Linux manuellement

**Avant de commencer :**

- Consultez la configuration requise pour CylancePROTECT Desktop.
- Téléchargez les fichiers d'installation à CylancePROTECT Desktop partir de la console de gestion. Cliquez sur **Paramètres > Déploiements**. Dans la liste déroulante **Produit**, sélectionnez **CylancePROTECT**, et définissez le système d'exploitation cible, la version de l'agent et le type de fichier. Cliquez sur **Télécharger**.
- Dans la console de gestion, copiez le jeton d'installation depuis **Paramètres > Application**.
- Vérifiez que vous disposez des autorisations root.

1. Créer un fichier de configuration pour l'installation de l'agent Linux.
2. Utilisez les commandes suivantes dans l'ordre indiqué pour installer le pilote et l'agent. Utilisez les fichiers extraits du fichier .tgz pour déterminer la valeur de *<version>*.

| Distribution Linux | Commandes |
|---|---|
| • Red Hat Enterprise Linux ou CentOS<br>• Amazon Linux<br>• Oracle<br>• SUSE Linux Enterprise Server | **a.** Installez le pilote d'ouverture :<br>`rpm -ivh CylancePROTECTOpenDriver-<version>.rpm`<br>**b.** Installez le pilote d'agent :<br>`rpm -ivh CylancePROTECTDriver-<version>.rpm`<br>**c.** Installez l'agent :<br>`rpm -ivh CylancePROTECT.<version>.rpm`<br>**d.** Installez l'interface utilisateur de l'agent* :<br>`rpm -ivh CylancePROTECTUI.<version>.rpm`<br>* Pour les terminaux exécutant SUSE Linux Enterprise Server, il est possible que vous deviez installer la bibliothèque Gnome 3 (libgtk-3-0) avant d'installer l'interface utilisateur de l'agent. Si nécessaire, utilisez la commande suivante : `zypper install libgtk-3-0` |

| Distribution Linux | Commandes |
| --- | --- |
| • Ubuntu<br>• Debian | **a.** Installez le pilote d'ouverture :<br>`dpkg -i cylance-protect-open-driver_<version>.deb`<br>**b.** Installez le pilote d'agent :<br>`dpkg -i cylance-protect-driver_<version>.deb`<br>**c.** Installez l'agent :<br>`dpkg -i cylance-protect.version.deb`<br>**d.** Installez l'interface utilisateur de l'agent :<br>`dpkg -i cylance-protect-ui.version.deb` |

**À la fin :**

Si l'interface utilisateur de l'agent ne démarre pas automatiquement après l'installation (par exemple, sur les terminaux CentOS, SUSE ou Ubuntu), vous devez redémarrer GNOME Shell pour afficher l'interface utilisateur CylancePROTECT. Consultez Démarrer l'interface utilisateur manuellement.

## Mettre à niveau le pilote Linux

Chaque kernel Linux pris en charge nécessite un pilote pris en charge pour que l'agent CylancePROTECT Desktop puisse s'exécuter sur le terminal. Lorsque vous mettez à niveau le kernel Linux sur un terminal, vous devez vous assurer que le terminal exécute un pilote qui le prend en charge. La mise à niveau du kernel vers la version la plus récente garantit que votre terminal reçoit les dernières mises à jour de sécurité du système d'exploitation, tandis que l'utilisation de l'agent et du pilote les plus récents garantit la protection de CylancePROTECT.

Vous disposez des options suivantes pour maintenir le pilote Linux à jour :

| Scénario | Actions |
| --- | --- |
| Mettez automatiquement à jour le pilote dès qu'une mise à jour est disponible lorsque vous mettez à niveau le noyau Linux | • Assurez-vous que les terminaux exécutent la version 3.1 ou versions ultérieures de l'agent et le pilote 3.1 ou versions ultérieures.<br>• Activez la fonctionnalité de mise à jour automatique du pilote Linux dans la règle de mise à jour. |

| Scénario | Actions |
| --- | --- |
| Mettez à jour manuellement le pilote lorsque vous mettez à niveau le kernel Linux | • Chaque fois que vous mettez à niveau le noyau Linux, vous devez télécharger manuellement le package de pilotes lorsqu'il est disponible dans la console de gestion. Pour déterminer la version minimale du pilote dont vous avez besoin pour le kernel Linux que vous utilisez, reportez-vous à la Feuille de calcul pilotes et kernels Linux pris en charge.<br>• Vous pouvez utiliser un gestionnaire de packages ou des outils et méthodes similaires pour mettre à jour l'agent et le pilote.<br>• Si vous choisissez de mettre à jour l'agent manuellement, BlackBerry vous recommande de modifier le paramètre de l'agent de mise à jour basé sur la zone sur Ne pas mettre à jour pour ces terminaux.<br>**Conseil :** Le pilote 3.1.1100 est compatible avec l'agent 2.1.1590 et les versions ultérieures. Vous pouvez installer le pilote sur les terminaux qui exécutent l'agent version 2.1.1590 ou versions ultérieures afin de bénéficier de la fonctionnalité de mise à jour automatique du pilote Linux lorsque vous effectuez une mise à niveau vers l'agent 3.1. |

#### Mettre à jour automatiquement le pilote Linux

Lorsque vous mettez à niveau le kernel Linux sur un terminal, vous devez vous assurer que le terminal exécute un pilote qui le prend en charge. Pour les terminaux exécutant l'agent CylancePROTECT Desktop 3.1 et versions ultérieures, vous pouvez activer la fonctionnalité de mise à jour automatique du pilote Linux, qui permet à l'agent de mettre automatiquement à jour le pilote lorsqu'un kernel mis à jour est détecté sur le système, dès qu'il est disponible. La mise à niveau du kernel vers la version la plus récente garantit que votre terminal reçoit les dernières mises à jour de sécurité du système d'exploitation, tandis que l'utilisation de l'agent et du pilote les plus récents garantit la protection de CylancePROTECT.

1. Dans la barre de menus de la console de gestion, accédez à **Paramètres > Mettre à jour**.
2. Cliquez sur une règle de mise à jour que vous utilisez pour gérer les mises à jour des terminaux Linux. Si vous devez en créer un, consultez Gérer les mises à jour pour les agents CylancePROTECT Desktop et CylanceOPTICS.
3. Développez la section **Agent**.
4. Sélectionnez l'option **Mise à jour automatique du pilote Linux**.
5. Cliquez sur **Enregistrer**.

#### Mise à jour manuelle du pilote Linux

Lorsque vous mettez à niveau le kernel sur votre terminal Linux, vous devez vous assurer que le terminal exécute un pilote qui le prend en charge. Lorsqu'une distribution Linux publie une mise à jour, BlackBerry crée un pilote Linux mis à jour et le rend disponible depuis la console de gestion. Un package de mise à jour de pilote est disponible uniquement s'il existe une version plus récente que celle incluse dans la version de l'agent.

BlackBerry recommande de mettre à niveau l'agent vers la version 3.1 ou ultérieures, ce qui active une fonctionnalité permettant à l'agent de mettre automatiquement à jour le pilote Linux après la détection d'un kernel mis à jour, dès qu'il est disponible. Si vous exécutez les versions 3.0 ou 2.1.1590 de l'agent, ou si vous choisissez de ne pas utiliser la fonction de mise à jour automatique du pilote Linux, vous devez installer manuellement un pilote pris en charge pour le kernel Linux. Vous pouvez utiliser les outils et méthodes de votre entreprise pour déployer les pilotes compatibles sur vos terminaux.

**Avant de commencer :**

- Vérifiez que vous disposez des autorisations root ou sudo.
- Déterminez la version minimale du pilote requise pour prendre en charge le kernel Linux sur votre terminal.

1. Sur la barre de menus de la console de gestion, cliquez sur **Paramètres > Déploiement**.
2. Dans la liste **Produit**, sélectionnez **Pilote CylancePROTECT**.
3. Dans la liste **Système d'exploitation**, sélectionnez le système d'exploitation pour lequel vous souhaitez télécharger le pilote.
4. Dans la liste **Version**, sélectionnez la version du pilote.
5. Dans la liste **Format**, sélectionnez le format du pilote.
6. Cliquez sur **Télécharger**.
7. Pour mettre à niveau le package RPM, utilisez l'une des commandes suivantes :

   Collez les deux pilotes dans la même ligne de commande et remplacez « xx » par le numéro de version du package :

| Distribution | Commandes |
|---|---|
| Oracle 6, Oracle UEK 6 | `rpm -Uvh CylancePROTECTOpenDriver-xx.el6.noarch.rpm CylancePROTECTDriver-xx.el6.noarch.rpm` |
| CentOS 7, RHEL 7, Oracle 7, Oracle UEK 7 | `rpm -Uvh CylancePROTECTOpenDriver-xx.el7.x86_64.rpm CylancePROTECTDriver-xx.el7.x86_64.rpm` |
| Amazon Linux 2 | `rpm -Uvh CylancePROTECTOpenDriver-xx.amzn2.x86_64.rpm CylancePROTECTDriver-xx.amzn2.x86_64.rpm` |
| SUSE Linux Enterprise Server | `rpm -Uvh CylancePROTECTOpenDriver-xx.x86_64.rpm CylancePROTECTDriver-xx.x86_64.rpm` |
| Prise en charge des distributions 32 bits Ubuntu et Xubuntu | • Installez les dépendances à l'aide de la commande suivante :<br>`apt-get update -y && apt-get install`<br>• Installez les packages DEB CylancePROTECT Desktop du pilote à l'aide des commandes suivantes :<br>`dpkg -i cylance-protect-open-driver_xx_i386_32.deb`<br>`dpkg -i cylance-protect-driver_xx_i386_32.deb` |

| Distribution | Commandes |
| --- | --- |
| Prise en charge des distributions 64 bits Ubuntu, Xubuntu et Debian | • Installez les dépendances à l'aide de la commande suivante :<br>`apt-get update -y && apt-get install`<br>• Installez les packages DEB CylancePROTECT Desktop du pilote à l'aide des commandes suivantes :<br>`dpkg -i cylance-protect-open-driver_xx_amd64.deb`<br>`dpkg -i cylance-protect-driver_xx_amd64.deb` |

8. Redémarrez le service à l'aide de la commande suivante : `systemctl start cylancesvc`.

### Commandes Linux de l'agent

Pour afficher la liste des commandes Linux de l'agent CylancePROTECT Desktop, procédez comme suit :

```
/opt/cylance/desktop/cylance -h
```

Exemple d'utilisation des commandes : `cylance <option>`

| Option | Description |
| --- | --- |
| -r, --register=<*token*> | Enregistrer l'agent auprès de la console à l'aide du jeton fourni |
| -s, --status | Rechercher les mises à jour de l'agent |
| -b, --start-bg-scan | Lancer l'analyse de détection des menaces en arrière-plan |
| -B, --stop-bg-scan | Arrêter l'analyse de détection des menaces en arrière-plan |
| -d, --scan-dir=<*dir*> | Analyser un répertoire |
| -l, --getloglevel | Récupérer le niveau de journalisation actuel |
| -L, --setloglevel=<*level*> | Définir le niveau de journalisation pour spécifier le niveau d'informations collectées dans les journaux de débogage |
| -P, --getpolicytime | Récupérer l'heure de mise à jour de la stratégie |
| -p, --checkpolicy | Rechercher des mises à jour de la stratégie |
| -t, --menaces | Afficher une liste des menaces |
| -q, --quarantine=<*id*> | Mettre un fichier en quarantaine en spécifiant un ID de hachage |
| -w, --waive=<*id*> | Ignorer un fichier en spécifiant un ID de hachage |
| -v, --version | Afficher la version de cet outil |
| -h, --help | Afficher une liste de commandes |

### Résolution des problèmes rencontrés lors de l'installation de l'agent Linux

Le tableau ci-dessous décrit les actions que vous pouvez effectuer pour résoudre les problèmes d'installation de l'agent Linux.

| Tâche ou erreur | Action |
|---|---|
| Démarrer ou arrêter le service d'agent | Utilisez les commandes suivantes pour démarrer ou arrêter le service Cylance sur un terminal Linux :<br>• Pour démarrer le service Cylance :<br>`systemctl start cylancesvc`<br>• Pour arrêter le service Cylance :<br>`systemctl stop cylancesvc` |
| Vérifier le chargement des pilotes du noyau | Pour vérifier si les pilotes du noyau sont chargés, saisissez la commande suivante :<br>`lsmod \| grep CyProtectDrv`<br>Si les modules de noyau sont chargés, la commande doit générer un résultat similaire au suivant :<br>`CyProtectDrv 210706  0CyProtectDrvOpen 16384 1 CyProtectDrv`<br>Si les modules du noyau ne sont pas chargés, aucune sortie n'est renvoyée. |
| Chargement et déchargement des pilotes du noyau | Sur l'agent CylancePROTECT Desktop Linux 2.1.1590 et les versions ultérieures, deux pilotes sont chargés et déchargés ensemble : `CyProtectDrv` et `CyProtectDrvOpen`. Sur les versions antérieures de l'agent, seul le pilote `CyProtectDrv` est chargé.<br>Pour charger les pilotes du noyau, saisissez l'une des commandes suivantes :<br>• Pour les distributions SUSE Linux :<br>`modprobe --allow-unsupported cyprotect`<br>Si vous ne souhaitez pas continuer à utiliser l'indicateur `--allow-unsupported`, modifiez `/etc/modprobe.d/10-unsupported-modules.conf` et remplacez « allow_unsupported_modules » par « 1 ».<br>• Pour toutes les autres distributions Linux :<br>`modprobe cyprotect` |
| Démarrer l'interface utilisateur Linux manuellement | Si l'interface utilisateur de l'agent ne démarre pas automatiquement après l'installation, consultez la section Démarrer l'interface utilisateur manuellement pour en savoir plus. |

| Tâche ou erreur | Action |
| --- | --- |
| Erreur : problèmes de version multilib détectés | Si le message « Erreur : problèmes de version multilib détectés » s'affiche lors de l'installation d'un package sur un terminal, consultez la section Erreur : problèmes de version multilib détectés pour en savoir plus. |

#### Démarrer l'interface utilisateur manuellement

Il est possible que l'interface utilisateur de l'agent ne démarre pas automatiquement après l'installation (par exemple, sur les terminaux CentOS, Ubuntu et SUSE. Pour la lancer manuellement, vous pouvez redémarrer l'extension GNOME Shell ou vous déconnecter, puis vous reconnecter.

L'outil GNOME Tweak doit être installé avant de redémarrer l'extension GNOME Shell. Il se peut qu'Ubuntu n'inclut pas l'outil GNOME Tweak par défaut.

1. Si vous devez installer l'outil GNOME Tweak, exécutez les commandes suivantes :

   ```
   add-apt-repository universe
   apt install gnome-tweak-tool
   ```

2. Pour redémarrer l'extension GNOME Shell, appuyez sur `Alt+F2`, saisissez « `r` » dans la boite de dialogue, puis appuyez sur la touche `ENTER`.
   Si l'icône CylanceUI n'apparaît pas, activez manuellement l'extension de GNOME Shell à partir de l'outil Tweak. Pour lancer l'outil GNOME Tweak, saisissez « `gnome-tweaks` » dans un terminal. Dans l'outil GNOME Tweak, accédez à l'onglet **Extensions** et activez l'interface utilisateur CylanceUI.

#### Erreur : problèmes de version multilib détectés

Si le message « Erreur : problèmes de version multilib détectés » s'affiche lors de l'installation d'un package sur un terminal exécutant Red Hat Enterprise Linux ou CentOS, cela signifie généralement que la bibliothèque 64 bits correspondante doit être installée ou mise à niveau avec la bibliothèque 32 bits. La vérification de version `multilib` indique simplement la présence d'un problème.

Par exemple, si l'erreur est liée à la bibliothèque `sqlite` :

- Il manque une dépendance requise par un autre package dans l'une des mises à niveau pour `sqlite`. `Yum` tente de résoudre ce problème en installant une ancienne version de `sqlite` de l'autre architecture. Si vous excluez l'autre architecture, `yum` affiche la cause première du problème, notamment des dépendances manquantes dans un package. Pour afficher un message d'erreur indiquant la cause première du problème, vous pouvez essayer de relancer la mise à niveau à l'aide de `--exclude sqlite.otherarch`.
- Vous avez installé plusieurs architectures de `sqlite`, mais `yum` ne peut détecter qu'une mise à niveau pour l'une d'entre elles. Si vous n'avez pas besoin des deux architectures, vous pouvez supprimer la version de `sqlite` sur laquelle la mise à jour de l'architecture est manquante et déterminer si l'erreur est résolue.
- Vous avez déjà installé des versions en double de `sqlite`. Vous pouvez utiliser « yum check » pour afficher ces erreurs.
- Pour installer ou mettre à niveau la bibliothèque `sqlite` correspondante, utilisez la commande suivante :

  ```
  yum install sqlite.i686 sqlite
  ```

  Si l'erreur est liée aux bibliothèques `dbus-libs`, `openssl` ou `libgcc`, remplacez `sqlite` par la bibliothèque appropriée dans la commande.

# Demander aux utilisateurs de fournir un mot de passe pour supprimer les agents CylancePROTECT Desktop et CylanceOPTICS

Vous pouvez demander aux utilisateurs de fournir un mot de passe pour désinstaller l'agent CylancePROTECT Desktop pour Windows et macOS, l'agent CylanceOPTICS pour Windows 3.1 ou ultérieure, ainsi que l'agent CylanceOPTICS pour macOS version 3.3 ou ultérieure. L'utilisation de cette fonctionnalité pour l'agent CylanceOPTICS sous macOS nécessite également CylancePROTECT Desktop version 3.1 ou ultérieure.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Application**.
2. Cochez la case **Exiger un mot de passe pour désinstaller l'agent**.
3. Spécifier un mot de passe.
4. Cliquez sur **Enregistrer**.

# Configurer CylancePROTECT Mobile

| Étape | Action |
|---|---|
| 1 | Consultez la configuration logicielle requise et la configuration réseau requise pour l'application CylancePROTECT Mobile. |
| 2 | Si vous souhaitez ajouter des utilisateurs CylancePROTECT Mobile à Cylance Endpoint Security depuis le répertoire d'entreprise, reportez-vous à la section Lier à votre répertoire d'entreprise. |
| 3 | Ajoutez des utilisateurs de l'application CylancePROTECT Mobile.<br>Vous pouvez également ajouter des groupes pour gérer les utilisateurs. |
| 4 | Création d'une stratégie CylancePROTECT Mobile. |
| 5 | Créer une stratégie d'inscription. |
| 6 | Les utilisateurs de terminaux installent et activent l'application CylancePROTECT Mobile. Pour obtenir des instructions, consultez le Guide de l'utilisateur Cylance Endpoint Security. |
| 7 | Vous pouvez éventuellement créer une stratégie d'évaluation des risques pour mapper les alertes sur les niveaux de risque des terminaux. Si vous n'attribuez pas de stratégie d'évaluation des risques personnalisée, une stratégie par défaut est appliquée aux utilisateurs de votre locataire. |
| 8 | Si vous le souhaitez, vous pouvez intégrer Cylance Endpoint Security à Microsoft Intune pour signaler les niveaux de risque des terminaux à Intune afin que Intune puisse exécuter les actions d'atténuation souhaitées sur les terminaux. |

Cylance Endpoint Security prend également en charge l'utilisation de stratégies de protection des applications Microsoft Intune pour autoriser ou restreindre l'accès à des applications Microsoft spécifiques en fonction du niveau de menace du terminal signalé par CylancePROTECT Mobile. Une autre série d'étapes de déploiement est nécessaire à l'activation de cette fonctionnalité. Pour configurer cette fonctionnalité, reportez-vous à la section Utiliser les stratégies de protection des applications Intune avec CylancePROTECT Mobile.

## Création d'une stratégie CylancePROTECT Mobile

Vous pouvez créer une stratégie et l'attribuer CylancePROTECT Mobile aux utilisateurs et aux groupes pour activer le service et contrôler les fonctionnalités que vous souhaitez utiliser.

**Avant de commencer :** Ajouter l'application CylancePROTECT Mobile et des utilisateurs CylanceGATEWAY.

1. Sur la barre de menus de la console de gestion, cliquez sur **Stratégies > Stratégie utilisateur**.
2. Dans l'onglet **Protect Mobile**, cliquez sur **Ajouter une stratégie**.
3. Saisissez le nom et la description de la stratégie.

4. Dans la section **Notifications**, vous pouvez spécifier le nombre et l'intervalle des notifications CylancePROTECT Mobile que l'application fournit à l'utilisateur lorsqu'elle détecte une menace. Vous spécifiez le type de notification (terminal, e-mail ou aucune notification) dans la section **Paramètres du terminal** (étape 6).
5. Dans la section **Confidentialité des données**, si vous souhaitez obfusquer certaines informations lorsque l'application CylancePROTECT Mobile signale une menace afin que les informations ne puissent pas être stockées et affichées dans la console de gestion en texte brut, activez **Confidentialité des données**, puis sélectionnez les champs que vous souhaitez masquer.
6. Dans la section **Paramètres du terminal**, cliquez sur **Android** ou **iOS** et activez les fonctions que vous souhaitez utiliser. Pour plus d'informations sur les fonctionnalités de CylancePROTECT Mobile, reportez-vous à la section Principales fonctionnalités de CylancePROTECT Mobile.
   a) Pour chaque fonctionnalité que vous activez, cochez la case appropriée pour activer ou désactiver les notifications du terminal et les notifications par e-mail. Si vous désactivez les notifications du terminal et par e-mail, l'utilisateur doit ouvrir l'application CylancePROTECT Mobile pour afficher les alertes.
   b) Si vous activez l'une des fonctions suivantes, procédez comme suit :

| Fonctionnalité | Plateforme | Étapes supplémentaires |
|---|---|---|
| Applications malveillantes | Android | **a.** Pour exempter les applications de la liste sécurisée de l'analyse anti-programmes malveillants, activez **Toujours autoriser les applications figurant dans la liste des applications sécurisées**.<br>**b.** Pour bloquer automatiquement les applications de la liste des applications dangereuses, activez **Toujours bloquer les applications figurant dans la liste des applications restreintes**.<br>**c.** Si vous souhaitez analyser les applications système préinstallées dans la partition système du terminal, activez l'option **Analyser les applications système**.<br>**d.** Si vous souhaitez activer le téléchargement d'applications vers les services CylancePROTECT Mobile via une connexion Wi-Fi, activez l'option **Télécharger les packages d'applications pour un contrôle de sécurité via une connexion Wi-Fi**. Spécifiez, en Mo, la taille maximale d'une application téléchargeable via une connexion Wi-Fi et la taille maximale de toutes les applications téléchargeables en un mois (30 jours). Si l'un des deux tailles maximales est dépassée, le téléchargement n'aura pas lieu et une erreur sera ajoutée au journal du terminal.<br>**e.** Si vous souhaitez activer le téléchargement d'applications vers les services CylancePROTECT Mobile via un réseau mobile, activez l'option **Télécharger les packages d'applications pour un contrôle de sécurité via une connexion réseau mobile**. Spécifiez, en Mo, la taille maximale d'une application téléchargeable via un réseau mobile et la taille maximale de toutes les applications téléchargeables en un mois (30 jours). Si l'un des deux tailles maximales est dépassée, le téléchargement n'aura pas lieu et une erreur sera ajoutée au journal du terminal. |

| Fonctionnalité | Plateforme | Étapes supplémentaires |
|---|---|---|
| Modèle de terminal non pris en charge | Android<br>iOS | Cliquez sur **Modifier** et sélectionnez les modèles de terminal que vous souhaitez restreindre. |
| Système d'exploitation non pris en charge | Android<br>iOS | Ajoutez les versions de système d'exploitation disponibles aux listes de prise en charge et de non-prise en charge en fonction des normes de sécurité de votre organisation. |
| Échec d'attestation SafetyNet ou Play Integrity | Android | Si vous souhaitez activer la correspondance Compatibility Test Suite mise pour l'application CylancePROTECT Mobile, activez **Activer la correspondance de profil CTS**. |
| Échec de l'attestation matérielle | Android | **a.** Dans la liste déroulante **Niveau de sécurité minimal requis**, cliquez sur le niveau approprié. Pour plus d'informations, reportez-vous à la page SecurityLevel sur le site d'Android Developers.<br>**b.** Si vous souhaitez appliquer un niveau de correctif de sécurité minimal sur les terminaux, activez **Niveau de correctif de sécurité**. Ajoutez les modèles de terminal appropriés et spécifiez la date du correctif de sécurité. |
| Wi-Fi non sécurisé | Android | Ajoutez les algorithmes d'accès Wi-Fi disponibles aux listes sécurisées et dangereuses en fonction des normes de sécurité de votre organisation. |
| Message dangereux | Android<br>iOS | **a.** Dans la liste déroulante **Option d'analyse**, sélectionnez l'une des options suivantes :<br>• Si vous souhaitez envoyer des messages aux services CylancePROTECT Mobile pour déterminer s'ils sont sécurisés, cliquez sur **Analyse dans le cloud**.<br>• Si vous souhaitez utiliser uniquement les modèles d'apprentissage automatique locaux de l'application CylancePROTECT Mobile pour identifier les URL dangereuses, cliquez sur **Analyse sur le terminal**.<br>• Si vous souhaitez désactiver l'analyse des URL, cliquez sur **Aucune analyse**.<br>**b.** Pour les terminaux Android, dans le champ **Décalage du début de l'analyse**, indiquez, en heures, la durée des messages texte pouvant être analysés. Si vous spécifiez 0, seuls les nouveaux messages peuvent être analysés. |

7. Cliquez sur **Ajouter**.

**À la fin :**

- Attribuer la stratégie à des utilisateurs et groupes.
- Si nécessaire, classez les stratégies.
- Créez une stratégie d'inscription et attribuez-la à des utilisateurs. Lorsqu'une stratégie d'inscription a été attribuée à des utilisateurs, ils reçoivent un e-mail contenant des instructions pour télécharger et activer l'application CylancePROTECT Mobile. Pour plus d'informations, consultez le Guide de l'utilisateur Cylance Endpoint Security.

    - Demandez aux utilisateurs d'activer JavaScript dans leur navigateur mobile par défaut (l'application CylancePROTECT Mobile prend en charge Google Chrome, Samsung Internet et Safari). Cela est nécessaire pour activer l'application CylancePROTECT Mobile.
    - Demandez aux utilisateurs Android d'autoriser l'activité en arrière-plan pour l'application CylancePROTECT Mobile après son installation.
- Vous pouvez éventuellement créer une stratégie d'évaluation des risques. Si vous ne créez pas et n'attribuez pas de stratégie d'évaluation des risques personnalisée, une stratégie par défaut est appliquée aux utilisateurs de votre locataire.

# Créer une stratégie d'évaluation des risques

Une stratégie d'évaluation des risques permet de mapper les alertes détectées par l'application CylancePROTECT Mobile sur les niveaux de risque (par exemple, vous pouvez indiquer que les terminaux compromis doivent être traités comme des terminaux à haut risque). Les niveaux de risque des alertes permettent de déterminer le niveau de risque global d'un terminal. Vous pouvez afficher le niveau de risque du terminal dans la console de gestion (Actifs > Terminaux mobiles et dans les détails du terminal).

Si vous ne créez pas de stratégie d'évaluation des risques, une stratégie par défaut est appliquée aux utilisateurs de votre locataire. Vous pouvez modifier la stratégie par défaut mais vous ne pouvez pas la supprimer.

Vous pouvez utiliser les stratégies d'évaluation des risques pour les fonctionnalités Cylance Endpoint Security suivantes :

- Si vous intégrez Cylance Endpoint Security à Microsoft Intune, Cylance Endpoint Security envoie périodiquement le niveau de risque global d'un terminal mobile à Intune. Vous pouvez utiliser Intune pour configurer des actions d'atténuation pour les niveaux de risque des terminaux.
- Vous pouvez prendre en compte le niveau de risque des terminaux mobiles dans les règles d'accès au réseau CylanceGATEWAY.

**Avant de commencer :** Configuration CylancePROTECT Mobile.

1. Sur la barre de menus de la console de gestion, cliquez sur **Stratégies > Stratégie d'utilisateur**.
2. Cliquez sur l'onglet **Évaluation des risques**.
3. Cliquez sur l'onglet **Ajouter une stratégie**.
4. Saisissez le nom et la description de la stratégie.
5. Dans la section **Évaluation des risques**, cliquez sur **Ajouter des détections > Détections**.
6. Faites glisser les détections vers le niveau de risque à appliquer à ces dernières.

   Pour plus d'informations sur les détections, reportez-vous à la section Principales fonctionnalités de CylancePROTECT Mobile.
7. Cliquez sur **Ajouter**.

**À la fin :**

- Attribuer la stratégie à des utilisateurs et groupes.
- Si nécessaire, classez les stratégies.
- Si vous le souhaitez, vous pouvez intégrer Cylance Endpoint Security à Intune pour répondre aux menaces mobiles.

# Intégration d'Cylance Endpoint Security à Microsoft Intune pour répondre aux menaces mobiles

Vous pouvez connecter Cylance Endpoint Security à Microsoft Intune afin qu'Cylance Endpoint Security puisse signaler le niveau de risque des terminaux à Intune. Le niveau de risque du terminal est calculé en fonction de la détection des menaces mobiles par l'application CylancePROTECT Mobile sur les terminaux gérés par Intune. Intune peut exécuter des actions d'atténuation en fonction du niveau de risque du terminal.

Lorsque vous vous connectez Cylance Endpoint Security à Intune, créez des stratégies de configuration d'application qui définissent les types de terminaux et les groupes Intune auxquels l'intégration s'applique. Créez et attribuez des stratégies d'évaluation des risques qui mappent des événements détectés par l'application CylancePROTECT Mobile au niveau de risque de votre choix (élevé, moyen ou faible). Lorsque l'application CylancePROTECT Mobile d'un terminal géré par Intune détecte une menace (par exemple, une application malveillante ou une application chargée latéralement), le niveau de risque associé à cette menace est pris en compte dans un niveau de risque global que Cylance Endpoint Security calcule pour le terminal. Cylance Endpoint Security signale le niveau de risque du terminal à Intune, et Intune exécute les actions de prévention configurées pour ce niveau de risque.

Notez que tous les terminaux gérés par Intune doivent être inclus dans une stratégie de configuration d'application dans la console Cylance. Cette fonctionnalité requiert l'application CylancePROTECT Mobile version 2.0.1.1099 ou ultérieure.

Cylance Endpoint Security prend également en charge l'utilisation de stratégies de protection des applications Microsoft Intune pour autoriser ou restreindre l'accès à des applications Microsoft spécifiques en fonction du niveau de menace du terminal signalé par CylancePROTECT Mobile. Pour activer cette fonctionnalité, consultez Utiliser les stratégies de protection des applications Intune avec CylancePROTECT Mobile.

## Connecter Cylance Endpoint Security à Intune

**Avant de commencer :** Le compte administrateur Cylance Endpoint Security que vous utilisez pour vous connecter à Intune doit disposer d'une licence Intune.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Connecteurs**.
2. Cliquez sur **Ajouter une connexion > Microsoft Intune**.
3. Indiquez votre ID de locataire Entra. Cliquez sur **Suivant**.
4. Spécifiez vos informations d'identification d'administrateur pour Entra.

   Suivez les invites pour obtenir le consentement de l'administrateur. Si nécessaire, contactez l'administrateur Intune de votre organisation pour qu'il accorde l'autorisation pour le connecteur MTD CylancePROTECT Mobile dans le centre d'administration Microsoft Intune.
5. Sur l'écran **Stratégies de configuration d'application**, activez les plateformes de système d'exploitation auxquelles appliquer l'intégration Intune et effectuez les étapes suivantes pour chaque plateforme. Tous les terminaux gérés par Intune avec lesquels vous utilisez cette fonctionnalité doivent être inclus dans une stratégie de configuration d'application. Pour créer des stratégies de configuration d'application ultérieurement, cliquez sur **Annuler**.
   a) Vous pouvez également modifier le nom de la stratégie. Ne modifiez pas l'application cible.
   b) Si vous souhaitez que la stratégie s'applique à tous les groupes de l'instance Intune, activez **Tous les groupes**.
   c) Si vous souhaitez que la stratégie s'applique à des groupes spécifiques de l'instance Intune, cliquez sur ⊕. Recherchez et sélectionnez des groupes, puis cliquez sur **Ajouter**.
6. Cliquez sur **Enregistrer**. Si vous avez ajouté une stratégie de configuration d'application pour Android, suivez les invites de consentement de l'administrateur qui s'affichent.

Les stratégies de configuration d'application que vous créez sont visibles dans le centre d'administration Intune.

**À la fin :**

- Si vous ne l'avez pas encore fait, créez une stratégie d'évaluation des risques pour faire correspondre les menaces détectées par l'application CylancePROTECT Mobile aux niveaux de risque souhaités.
- Dans le centre d'administration Intune, modifiez le connecteur MTD CylancePROTECT Mobile et activez les options de stratégie de conformité pour connecter les terminaux Android et iOS à CylancePROTECT.

# Utiliser les stratégies de protection des applications Intune avec CylancePROTECT Mobile

Vous pouvez utiliser des stratégies de protection des applications Microsoft Intune avec CylancePROTECT Mobile pour autoriser ou restreindre l'accès à des applications Microsoft spécifiques en fonction du niveau de menace du terminal signalé par CylancePROTECT Mobile.

1. Consultez la configuration logicielle requise et la configuration réseau requise pour l'application CylancePROTECT Mobile.
2. Liez Cylance Endpoint Security à l'annuaire de votre entreprise.
3. Ajoutez les utilisateurs Intune à Cylance Endpoint Security en tant qu'utilisateurs CylancePROTECT Mobile.
4. Créez une stratégie CylancePROTECT Mobile et attribuez-la aux utilisateurs.
5. Créez une stratégie d'inscription et attribuez-la aux utilisateurs.

   Les utilisateurs recevront un e-mail contenant des instructions pour télécharger et activer l'application CylancePROTECT Mobile. Demandez aux utilisateurs d'ignorer l'e-mail pour le moment. Ils téléchargeront et activeront l'application à l'étape 10. Demandez aux utilisateurs de conserver l'e-mail car ils auront besoin du code QR pour activer l'application CylancePROTECT Mobile.
6. Créez une stratégie d'évaluation des risques pour mapper les alertes sur les niveaux de risque des terminaux. Si vous n'attribuez pas de stratégie d'évaluation des risques personnalisée, une stratégie par défaut est appliquée aux utilisateurs de votre locataire.
7. Connecter Cylance Endpoint Security à Intune.
8. Dans le centre d'administration Intune :
   a) Modifiez le connecteur MTD CylancePROTECT Mobile et activez les options de stratégie de protection des applications pour connecter les terminaux Android et iOS à CylancePROTECT.
   b) Créez et configurez des stratégies de protection des applications pour les terminaux Android et iOS et afin de spécifier la manière dont vous souhaitez que CylancePROTECT Mobile autorise ou restreigne l'accès à des applications spécifiques en fonction du niveau de risque signalé.
   c) Attribuer des stratégies de protections des applications à des groupes d'utilisateurs.
9. Déployez les applications Microsoft que vous souhaitez protéger à l'aide de la stratégie de protection des applications de Intune. Après l'installation d'une application Microsoft protégée, les utilisateurs sont invités à installer l'application Microsoft Authenticator (iOS) ou l'application du portail de l'entreprise Intune () Android et à enregistrer le terminal.
10. Demandez aux utilisateurs de lancer une application Microsoft protégée et de suivre l'invite « Obtenir l'accès » pour installer et activer l'application CylancePROTECT Mobile. Demandez aux utilisateurs d'utiliser le QR Code qu'ils ont reçu à l'étape 5.

    Si les utilisateurs Android ne reçoivent pas l'invite d'installation de l'application CylancePROTECT Mobile, demandez-leur de fermer et d'ouvrir à nouveau l'application Microsoft protégée.

Lorsqu'un utilisateur ouvre une application Microsoft protégée, il reçoit une notification si l'accès à l'application est restreint en raison du niveau de risque actuel du terminal.

# Configurer CylanceOPTICS

| Étape | Action |
|---|---|
| 1 | Consultez la Configuration logicielle requise. |
| 2 | Installer l'agent CylanceOPTICSsur des terminaux. |
| 3 | Activer et configurer CylanceOPTICS. |
| 4 | Gérer les mises à jour pour les agents CylancePROTECT Desktop et CylanceOPTICS. |

## Installer l'agent CylanceOPTICSsur des terminaux

Pour activer un terminal pour CylanceOPTICS, vous devez installer l'agent CylanceOPTICSsur le terminal. Téléchargez le programme d'installation de l'agent CylanceOPTICSà partir de la console de gestion, puis exécutez-le sur les terminaux en utilisant la méthode choisie par votre organisation. Par exemple, vous pouvez demander aux administrateurs informatiques de préinstaller l'agent sur les terminaux avant de les fournir aux utilisateurs, ou vous pouvez envoyer l'installation à l'aide d'un processus de distribution logicielle fiable.

**Avant de commencer :**

- Consultez la configuration logicielle requise pour CylanceOPTICS.
- Vous devez installer l'agent CylancePROTECT Desktopsur les terminaux avant d'installer l'agent CylanceOPTICS.
- Si vous souhaitez installer l'agent CylanceOPTICSsur des terminaux macOSBig Sur (11.x) ou une version ultérieure , reportez-vous à la page Configuration requise pour macOS 11.x et versions ultérieures.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Déploiements**.
2. Dans la liste déroulante **Produit**, cliquez sur **CylanceOPTICS**.
3. Sélectionnez le système d'exploitation, la version et le format.

   **Remarque :**

   - Pour les terminaux macOS, il est recommandé d'utiliser le fichier .pkg. Le fichier .dmg est une image disque du fichier .pkg qui peut être utilisée lorsqu'une image disque doit être montée pour l'installation.
   - Avant de déployer l'agent sur des terminaux macOS, reportez-vous à l'article 66578 de la base de connaissances : Autorisation des extensions du noyau Cylance à résoudre le problème « #Échec de connexion du pilote ».
   - Pour les terminaux avec serveur Oracle Linux UEK 8 et Oracle Linux 8, utilisez le fichier d'installation Oracle 8 (nécessite l'agent CylanceOPTICS 3.2 ou une version ultérieure).
4. Cliquez sur **Télécharger**.
5. À l'aide de la méthode de distribution logicielle préférée de votre organisation, déployez et exécutez le fichier d'installation sur les terminaux.

Si vous souhaitez installer l'agent CylanceOPTICSsur des terminaux Windowsou macOSà l'aide de commandes de SE, ou si vous effectuez l'installation sur Linux, reportez-vous à la page Commandes du système d'exploitation pour l'agent CylanceOPTICS.

**À la fin :**

- Activez et configurez CylanceOPTICSdans une stratégie de terminal et attribuez la stratégie à une ou plusieurs zones.
- Pour plus d'informations sur la gestion des mises à niveau de l'agent CylanceOPTICS, consultez Gérer les mises à jour pour les agents CylancePROTECT Desktop et CylanceOPTICS.

## Configuration requise pour macOS 11.x et versions ultérieures

Pour installer l'agent CylanceOPTICS version 3.0 ou ultérieure sur les terminaux dotés de macOS Big Sur (11.x) ou version ultérieure, notez les exigences de configuration suivantes. Les exigences varient selon que les terminaux sont gérés par une solution MDM (par exemple, Jamf Pro).

#### Terminaux gérés par MDM

Les informations ci-dessous utilisent Jamf Pro comme solution MDM, mais elles s'appliquent à d'autres solutions MDM.

| Configuration requise | Étapes |
|---|---|
| Activez l'accès complet au disque pour CylanceOPTICS. | Créez un profil de configuration et configurez les préférences de confidentialité suivantes :<br>• Identifiant : com.Cylance.Optics<br>• Type d'identifiant : ID de lot<br>• Exigence de code :<br>`identifier "com.cylance.Optics" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = "6ENJ69K633"`<br>• SystemPolicyAllFiles service : autoriser |
| Activez l'extension système CylanceOPTICS. | Créez un profil de configuration et configurez les préférences de confidentialité suivantes :<br>• Nom d'affichage : extension du système Optics Cylance EndPoint Security<br>• Types d'extension système : extensions système autorisées<br>• Identifiant de l'équipe : 6ENJ69K633<br>• Extensions système autorisées : com.cylance.CyOpticsESF.extension |

| Configuration requise | Étapes |
| --- | --- |
| Activez l'accès complet au disque de l'extension système CylanceOPTICS. | Créez un profil de configuration et configurez les préférences de confidentialité suivantes :<br>• Identifiant : com.cylance.CyOpticsESF.extension<br>• Type d'identifiant : ID de lot<br>• Exigence de code :<br>`anchor apple generic and identifier "com.cylance.CyOpticsESF.extension" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = "6ENJ69K633")`<br>• SystemPolicyAllFiles service : autoriser |
| Activez l'extension réseau CylanceOPTICS. | Créez un profil de configuration et configurez les paramètres de filtre de contenu suivants :<br>• Nom du filtre : com.cylance.CyOpticsESF.extension<br>• Identifiant : com.cylance.CyOpticsESF.extension<br>• Identifiant de bundle de filtres de socket : com.cylance.CyOpticsESF.extension<br>• Exigence désignée pour le filtre de socket :<br>`anchor apple generic and identifier "com.cylance.CyOpticsESF.extension" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = "6ENJ69K633")`<br>• Identifiant de bundle de filtres réseau : com.cylance.CyOpticsESF.extension<br>• Exigence désignée pour le filtre réseau :<br>`anchor apple generic and identifier "com.cylance.CyOpticsESF.extension" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = "6ENJ69K633")` |
| Redémarrez après l'installation. | Après avoir effectué les étapes de configuration ci-dessus et installé l'agent CylanceOPTICS, redémarrez le terminal. |

#### Terminaux qui ne sont pas gérés par MDM

Après avoir installé l'agent CylanceOPTICS :

1. Redémarrez le terminal.
2. Accédez aux paramètres de sécurité et de confidentialité et approuvez CyOpticsESFLoader.

3. Lorsque vous y êtes invité, autorisez le filtre réseau CylanceOPTICS.
4. Si la protection de l'intégrité du système (SIP) est activée sur le terminal, dans l'onglet Confidentialité, cliquez sur Accès complet au disque et vérifiez que CyOpticsESFLoader est sélectionné. Si CyOpticsESFLoader ne figure pas dans la liste, cliquez sur +, accédez à /Library/Application Support/Cylance/Optics, puis sélectionnez CyOptics.
5. Redémarrez le terminal.

Pour vérifier que l'extension du système est chargée :

1. Exécutez `$ systemextensionsctl list` et vérifiez que la sortie inclut `com.Cylance.CyOpticseSF.extension`.
2. Exécutez `$ ps aux | grep -i extension | grep -i Cylance` et vérifiez que la sortie inclut `com.cylance.CyOpticsESF.extension.systemextension`.

## Commandes du système d'exploitation pour l'agent CylanceOPTICS

Le programme d'installation de l'agent CylanceOPTICS prend en charge les commandes de système d'exploitation suivantes.

#### Windows

| Actions | Commandes |
|---|---|
| Spécifiez le répertoire d'installation. | `INSTALLFOLDER=<path>` |
| Spécifiez le répertoire du magasin de données local CylanceOPTICS. | `OPTICSROOTDATAFOLDER=<path>` |
| Effectuez une installation silencieuse sans intervention de l'utilisateur. | Pour le paquet .exe, utilisez l'un des éléments suivants :<br>• `-q`<br>• `-quiet`<br>• `-s`<br>• `-silent`<br>Pour le paquet .msi, utilisez l'un des éléments suivants :<br>• `/q`<br>• `/quiet` |
| Créez un fichier journal d'installation. | Pour le paquet .exe, utilisez l'un des éléments suivants :<br>• `-l <path_for_log>`<br>• `-log <path_for_log>`<br>Pour le paquet .msi, utilisez l'un des éléments suivants :<br>• `/l <path_for_log>`<br>• `/log <path_for_log>` |

| Actions | Commandes |
|---|---|
| Désactivez le contournement du proxy pour l'agent CylanceOPTICS (package .msi uniquement). | Utilisez cette option si vous souhaitez que l'agent CylanceOPTICS utilise toujours une connexion proxy spécifiée aux services cloud CylanceOPTICS. Cette option est facultative dans la plupart des environnements, mais nécessaire si vous utilisez CylanceHYBRID.<br><br>Avant d'exécuter le programme d'installation à l'aide de la commande ci-dessous, créez la clé de registre ProxyServer sur le terminal. Consultez Configuration d'un proxy pour les agents CylancePROTECT Desktop et Cylance OPTICS. Si vous utilisez CylanceHYBRID, reportez-vous aux instructions de configuration Windows du Guide d'administration CylanceHYBRID et créez la clé de registre ProxyServer avec la valeur requise pour CylanceHYBRID.<br><br>Après avoir créé la clé de registre ProxyServer sur le terminal, utilisez la commande suivante lors de l'installation de l'agent : `HYBRID=True`<br><br>Le programme d'installation crée la clé de registre DisableProxyBypass sur le terminal avec la valeur définie sur True. Pour plus d'informations, consultez Options de proxy pour l'agent CylanceOPTICS. Si la commande est définie sur `False`, le programme d'installation ne crée pas la clé de registre. |
| Désinstaller l'agent CylanceOPTICS. | `"<CylanceOPTICS_program_directory>\CyOpticsUninstaller.exe"`<br><br>Par exemple : `"C:\Program Files\Cylance\Optics \CyOpticsUninstaller.exe"`<br><br>Pour effectuer une désinstallation en mode silencieux sans intervention de l'utilisateur, ajoutez les commandes suivantes : `--use_cli -t v20`<br><br>Si vous avez configuré l'agent CylanceOPTICS pour exiger un mot de passe de désinstallation, ajoutez la commande suivante : `--password <password>`<br><br>Par exemple : `"C:\Program Files\Cylance\Optics \CyOpticsUninstaller.exe" --use_cli -t v20 --password samplepass` |

**macOS**

| Action | Commandes |
|---|---|
| Installer l'agent CylanceOPTICS. | `sudo installer -pkg CylanceOPTICS.pkg -target /` |
| Installer l'agent CylanceOPTICS et créez un fichier journal d'installation. | `sudo installer -verboseR -dumplog -pkg CylanceOPTICS.pkg -target /` |

| Action | Commandes |
|---|---|
| Désactivez le contournement du proxy pour l'agent CylanceOPTICS | Utilisez cette option si vous souhaitez que l'agent CylanceOPTICS utilise toujours une connexion proxy spécifiée aux services cloud CylanceOPTICS. Cette option est facultative dans la plupart des environnements, mais nécessaire si vous utilisez CylanceHYBRID.<br>Avant d'installer l'agent CylanceOPTICS, suivez les instructions de la section Conditions requises pour le proxy Cylance Endpoint Security pour configurer le contournement du proxy pour les terminaux macOS. |
| Démarrer le service CylanceOPTICS. | `sudo launchctl load /Library/LaunchDaemons/com.cylance.cyoptics_service.plist` |
| Arrêter le service CylanceOPTICS. | `sudo launchctl unload /Library/LaunchDaemons/com.cylance.cyoptics_service.plist` |
| Désinstaller l'agent CylanceOPTICS. | `sudo /Applications/Cylance/Optics/Uninstall\ CylanceOPTICS.app/Contents/MacOS/Uninstall\ CylanceOPTICS` |
| Désinstaller l'agent CylanceOPTICS sans interface utilisateur. | `sudo /Applications/Cylance/Optics/Uninstall\ CylanceOPTICS.app/Contents/MacOS/Uninstall\ CylanceOPTICS --noui`<br>Si vous souhaitez utiliser cette commande, des actions supplémentaires sont requises sur les terminaux macOS 11.x. Pour plus d'informations, reportez-vous à la section Résolution des problèmes du contenu Administration Cylance. |

**Linux**

| Action | Commandes |
|---|---|
| Installez l'agent CylanceOPTICS sur RHEL/CentOS, SUSE ou Amazon Linux 2. | `yum install CylanceOPTICS-<version>.rpm`, où <version> correspond à la version du fichier .rpm. |
| Installez l'agent CylanceOPTICS sur Ubuntu. | `dpkg -i cylance-optics_<version>_amd64.deb`, où <version> correspond à la version du fichier .deb. |
| Démarrer le service CylanceOPTICS. | `systemctl start cyoptics.service` |
| Arrêter le service CylanceOPTICS. | `systemctl stop cyoptics.service` |
| Désinstaller l'agent CylanceOPTICS sur RHEL/CentOS, SUSE ou Amazon Linux 2. | `rpm -e CylanceOPTICS` |

| Action | Commandes |
| --- | --- |
| Désinstaller l'agent CylanceOPTICS pour Ubuntu. | `dpkg -P cylance-optics` |

# Activer et configurer CylanceOPTICS

Lorsque vous activez CylanceOPTICS dans une stratégie de terminal et attribuez cette stratégie aux terminaux et aux zones, l'agent CylanceOPTICS de chaque terminal collecte les événements et stocke les données dans la base de données CylanceOPTICS. L'agent ne collecte pas de données tant que vous n'avez pas activé CylanceOPTICS.

**Avant de commencer :** Vérifiez que la fonction de contrôle d'application de CylancePROTECT Desktop n'est pas activée. Le contrôle d'application est conçu pour les dispositifs à fonction fixe qui ne changent pas après la configuration (par exemple, les machines de point de vente). Si le contrôle d'application est activé, l'agent CylanceOPTICS ne fonctionnera pas comme prévu.

1. Sur la barre de menus de la console de gestion, cliquez sur **Stratégies > Stratégie de terminal**.
2. Créez une nouvelle stratégie ou cliquez sur une stratégie existante.
3. Dans l'onglet **Paramètres CylanceOPTICS**, cochez la case **CylanceOPTICS**.
4. Si vous souhaitez activer le téléchargement automatique des données de cible liées aux menaces depuis la base de données CylanceOPTICS vers la console, dans la section **Menaces**, cochez la case **Chargement automatique**.

   Si vous ne sélectionnez pas cette option, vous devez utiliser la console pour demander des données détaillées pour les terminaux.
5. Si vous souhaitez activer le téléchargement automatique des données détaillées liées à la mémoire depuis la base de données CylanceOPTICS vers la console, cochez la case **Chargement automatique** dans la section **Protection de la mémoire**.

   Si vous ne sélectionnez pas cette option, vous devez utiliser la console pour demander des données détaillées pour les terminaux.
6. Dans la section **Capteurs configurables**, sélectionnez les capteurs CylanceOPTICS en option à activer. Notez que les capteurs en option sont pris en charge pour les systèmes d'exploitation 64 bits uniquement.
7. Dans le champ **Définir le stockage maximal du terminal**, spécifiez la quantité maximale de stockage, en Mo, à laquelle l'agent CylanceOPTICS peut accéder sur chaque terminal. La valeur par défaut est de 1 000 Mo.
8. Si vous souhaitez autoriser l'agent CylanceOPTICS à fournir des notifications de système d'exploitation à l'utilisateur sur les terminaux Windows ou macOS, cochez la case **Activer les notifications CylanceOPTICS Bureau**.
9. Si vous souhaitez associer un jeu de règles de détection à la stratégie de terminal, cliquez sur un jeu de règles dans la liste déroulante **Sélectionner un jeu de détection**.
10. Cliquez sur **Créer** ou **Enregistrer**.

    Si vous modifiez une stratégie existante et que vous souhaitez enregistrer les paramètres actuels en tant que nouvelle stratégie de terminal, cliquez sur **Enregistrer sous** à la place.

**À la fin :**

- Attribuer une stratégie à des terminaux ou des zones.
- Si vous voulez empêcher les utilisateurs de pouvoir arrêter les services de l'agent CylanceOPTICS pour Windows (CylanceOPTICS 3.1 ou versions ultérieures avec CylancePROTECT Desktop 3.0 ou versions ultérieures) et macOS (CylanceOPTICS 3.3 ou versions ultérieures avec CylancePROTECT Desktop 3.1 ou

versions ultérieures), dans la stratégie de terminal, sous **Paramètres de protection**, activez **Empêcher l'arrêt du service à partir du terminal**. Lorsque ce paramètre est activé, un utilisateur macOS ne peut arrêter le service que si le niveau d'autoprotection dans les propriétés du terminal est défini sur Admin local (Actifs > Terminaux > cliquez sur le terminal). Les utilisateurs Windows ne peuvent pas arrêter le service de l'agent tant que ce paramètre est activé.

- Si vous voulez que les utilisateurs aient à fournir un mot de passe pour désinstaller l'agent CylancePROTECT Desktop, l'agent CylanceOPTICS pour Windows version 3.1 ou versions ultérieures et l'agent CylanceOPTICS pour macOS version 3.3 ou versions ultérieures, dans **Paramètres > Application**, activez **Exiger un mot de passe pour désinstaller l'agent**. L'utilisation de cette fonctionnalité pour l'agent CylanceOPTICS sous macOS nécessite également CylancePROTECT Desktop version 3.1 ou ultérieure.

## Capteurs CylanceOPTICS

Les capteurs suivants sont activés par défaut dans l'agent CylanceOPTICS lorsque vous activez CylanceOPTICS dans une stratégie de terminal. Vous ne pouvez pas désactiver ces capteurs. Pour plus d'informations sur les capteurs facultatifs que vous pouvez activer, reportez-vous à la section Capteurs CylanceOPTICS en option.

Pour plus d'informations sur les évènements, les artéfacts et les types d'évènements associés aux capteurs par défaut et facultatifs, reportez-vous à la section Structures de données utilisées par CylanceOPTICS pour identifier les menaces.

| Capteur | Plateforme | Description | Types d'évènements |
|---|---|---|---|
| Terminal | macOS<br>Linux | Collecte des informations pertinentes sur le terminal. | Monter |
| Fichier | Windows<br>macOS<br>Linux | Collecte des informations relatives à des opérations sur fichier. | • Créer<br>• Supprimer<br>• Écraser<br>• Renommer<br>• Écrire |
| Mémoire | macOS<br>Linux | Collecte des informations relatives à des opérations sur mémoire. | • Mmap<br>• MProtect |
| Réseau | Windows<br>macOS<br>Linux | Collecte des informations sur les connexions réseau. | Se connecter |

| Capteur | Plateforme | Description | Types d'évènements |
|---|---|---|---|
| Processus | Windows<br>macOS<br>Linux | Collecte des informations sur des opérations de processus. | Les types d'évènement pris en charge varient en fonction de la plateforme. Reportez-vous à la section Processus de Structures de données utilisées par CylanceOPTICS pour identifier les menaces.<br>• Sortie anormale<br>• Quitter<br>• Sortie forcée<br>• PTrace<br>• Démarrer<br>• Suspendre<br>• Évènement de processus Linux inconnu |
| Registre | Windows | Collecte des informations sur les opérations de registre. | • KeyCreated<br>• KeyDeleting<br>• ValueChanging<br>• ValueDeleting |

### Capteurs CylanceOPTICS en option

Vous pouvez activer l'un des capteurs CylanceOPTICS suivants pour collecter des données supplémentaires, outre les évènements de processus, de fichiers, de réseau et des évènements de registre. L'activation de capteurs facultatifs peut avoir un impact sur les performances et l'utilisation des ressources sur les terminaux, ainsi que sur la quantité de données stockées dans la base de données CylanceOPTICS. BlackBerry recommande d'activer les capteurs facultatifs sur un petit nombre de terminaux pour évaluer l'impact.

Les capteurs facultatifs sont pris en charge pour les systèmes d'exploitation 64 bits uniquement, sauf mention contraire.

| Capteur | Description | Bonnes pratiques | Notes |
|---|---|---|---|
| Visibilité avancée des scripts | L'agent CylanceOPTICS enregistre les commandes, les arguments, les scripts et le contenu à partir de JScript, PowerShell (console et environnement de script intégré), VBScript et l'exécution de script de macro VBA.<br>Ratio signal/bruit : Élevé<br>Impact potentiel sur la conservation des données et les performances : Faible à modéré | Recommandé pour :<br>• Ordinateurs de bureau<br>• Ordinateurs portables<br>• Serveurs<br>Non recommandé pour Microsoft Exchange et les serveurs de messagerie. | • Les outils fournis par Microsoft ou d'autres solutions tierces peuvent considérablement dépendre de PowerShell pour réaliser les opérations.<br>• Pour améliorer la conservation des données, BlackBerry vous recommande de configurer des exceptions de détection pour les outils fiables qui utilisent beaucoup PowerShell. |

| Capteur | Description | Bonnes pratiques | Notes |
|---|---|---|---|
| Visibilité WMI avancée | L'agent CylanceOPTICS enregistre les attributs et paramètres WMI supplémentaires.<br>Ratio signal/bruit : Élevé<br>Impact potentiel sur la conservation des données et les performances : Faible | Recommandé pour :<br>• Ordinateurs de bureau<br>• Ordinateurs portables<br>• Serveurs | • Certains processus d'arrière-plan et de maintenance Windows utilisent WMI pour planifier des tâches ou exécuter des commandes, ce qui peut entrainer des pics d'activité WMI élevée.<br>• BlackBerry recommande d'analyser l'utilisation WMI dans votre environnement avant d'activer ce capteur. |
| Capteur API | L'agent CylanceOPTICS surveille un ensemble identifié d'appels d'API Windows.<br>Ratio signal/bruit : Modéré<br>Impact potentiel sur la rétention des données et les performances : l'activation de ce capteur peut avoir un impact sur les performances du processeur d'un terminal | Recommandé pour :<br>• Ordinateurs de bureau<br>• Ordinateurs portables<br>• Serveurs | • Pris en charge sur les systèmes d'exploitation Windows x86 ou x64.<br>• Nécessite l'agent CylancePROTECT Desktop 3.0.1003 ou une version ultérieure.<br>• Nécessite l'agent CylanceOPTICS 3.2 ou une version ultérieure. |
| Visibilité de l'objet COM | L'agent CylanceOPTICS surveille les appels d'API et d'interface COM pour détecter les comportements malveillants tels que la création de tâches planifiées.<br>Ratio signal/bruit : Élevé<br>Impact potentiel sur la rétention des données et les performances : l'activation de ce capteur peut avoir un impact sur les performances du processeur. | Recommandé pour :<br>• Ordinateurs de bureau<br>• Ordinateurs portables<br>Non recommandé pour les serveurs. | • Windows uniquement.<br>• Nécessite l'agent CylancePROTECT Desktop 3.2 ou une version ultérieure.<br>• Nécessite l'agent CylanceOPTICS 3.3 ou une version ultérieure. |

| Capteur | Description | Bonnes pratiques | Notes |
|---|---|---|---|
| Détection de cryptojacking | L'agent CylanceOPTICS traite l'activité de l'UC Intel à l'aide de registres matériels à la recherche d'activités potentielles de minage de cryptomonnaie et de cryptojacking.<br>Ratio signal/bruit : Modéré<br>Impact potentiel sur la conservation des données et les performances : Faible | Système d'exploitation pris en charge :<br>• Windows 10 x64<br>• Intel génération 6 à 10 | **Remarque :** BlackBerry recommande de désactiver ce capteur, car nous étudions actuellement les problèmes de stabilité que ce capteur peut causer avec le système d'exploitation du terminal.<br>• Non pris en charge pour les machines virtuelles.<br>• Non pris en charge pour les processeurs Intel de génération 11 ou ultérieure. BlackBerry ne recommande pas l'activation de ce capteur pour la génération 11 ou ultérieure. |
| Visibilité DNS | L'agent CylanceOPTICS enregistre les requêtes DNS, les réponses et les champs de données associés tels que Nom de domaine, Adresses résolues et Type d'enregistrement.<br>Ratio signal/bruit : Modéré<br>Impact potentiel sur la conservation des données et les performances : Modéré | Recommandé pour :<br>• Ordinateurs de bureau<br>• Ordinateurs portables<br>Non recommandé pour les serveurs DNS. | • Notez que ce capteur peut collecter une quantité importante de données, mais peut également fournir une visibilité sur les données que d'autres outils peinent à enregistrer.<br>• Pour améliorer la conservation des données, BlackBerry vous recommande de configurer des exceptions de détection pour les outils fiables qui utilisent beaucoup les services cloud. |

| Capteur | Description | Bonnes pratiques | Notes |
|---|---|---|---|
| Visibilité améliorée de la lecture des fichiers | L'agent CylanceOPTICS surveille les lectures de fichiers dans un ensemble identifié de répertoires.<br>Ratio signal/bruit : Modéré<br>Impact potentiel sur la conservation des données et les performances : Faible | Recommandé pour :<br>• Ordinateurs de bureau<br>• Ordinateurs portables<br>• Serveurs | • Certains outils de sécurité tiers peuvent utiliser les API Windows à partir desquelles ce capteur collecte des données. Dans certains cas, CylanceOPTICS peut enregistrer des données non pertinentes ou fiables.<br>• Pour améliorer la conversation des données et obtenir un ratio signal/bruit plus élevé, BlackBerry recommande de configurer des exceptions de détection pour des outils de sécurité fiables. |
| Analyse améliorée de fichiers exécutables portables | L'agent CylanceOPTICS enregistre les champs de données associés aux fichiers exécutables portables, tels que la version de fichier, les fonctions d'importation et les types d'outils Packer.<br>Ratio signal/bruit : Modéré<br>Impact potentiel sur la conservation des données et les performances : Faible | Recommandé pour :<br>• Ordinateurs de bureau<br>• Ordinateurs portables<br>• Serveurs | • Les données collectées par ce capteur sont transmises au moteur d'analyse de contexte pour faciliter l'analyse avancée des fichiers exécutables et ne sont pas stockées dans la base de données CylanceOPTICS.<br>• L'activation de ce capteur aura peu ou pas d'impact sur la conservation des données CylanceOPTICS.<br>• Si vous ajoutez et activez une règle de détection qui analyse les ressources de chaîne, l'agent CylanceOPTICS peut consommer d'importantes ressources de processeur et de mémoire. |

| Capteur | Description | Bonnes pratiques | Notes |
|---|---|---|---|
| Visibilité Améliorée des processus et de l'accrochage | L'agent CylanceOPTICS enregistre les informations de processus à partir des messages d'API Win32 et d'audit de noyau pour détecter les formes d'accrochage et d'injection de processus.<br>Ratio signal/bruit : Modéré<br>Impact potentiel sur la conservation des données et les performances : Faible | Recommandé pour :<br>• Ordinateurs de bureau<br>• Ordinateurs portables<br>• Serveurs | • Certains outils de sécurité tiers peuvent utiliser les API Windows à partir desquelles ce capteur collecte des données. Dans certains cas, CylanceOPTICS peut enregistrer des données non pertinentes ou fiables.<br>• Pour améliorer la conversation des données et obtenir un ratio signal/bruit plus élevé, BlackBerry recommande de configurer des exceptions de détection pour des outils de sécurité fiables. |
| Visibilité HTTP | L'agent CylanceOPTICS suit les transactions HTTP Windows, y compris le suivi des événements pour Windows, les API WinINet et les API WinHTTP.<br>Ratio signal/bruit : Élevé<br>Impact potentiel sur la rétention des données et les performances : l'activation de ce capteur peut avoir un impact sur les performances du processeur. | Recommandé pour :<br>• Ordinateurs de bureau<br>• Ordinateurs portables<br>Non recommandé pour les serveurs. | • Windows uniquement.<br>• Nécessite l'agent CylancePROTECT Desktop 3.2 ou une version ultérieure.<br>• Nécessite l'agent CylanceOPTICS 3.3 ou une version ultérieure. |
| Visibilité de la charge du module | L'agent CylanceOPTICS surveille les charges du module.<br>Ratio signal/bruit : Élevé<br>Impact potentiel sur la rétention des données et les performances : l'activation de ce capteur peut avoir un impact sur les performances du processeur. | Recommandé pour :<br>• Ordinateurs de bureau<br>• Ordinateurs portables<br>• Serveurs | • Windows uniquement.<br>• Nécessite l'agent CylancePROTECT Desktop 3.2 ou une version ultérieure.<br>• Nécessite l'agent CylanceOPTICS 3.3 ou une version ultérieure. |

| Capteur | Description | Bonnes pratiques | Notes |
|---|---|---|---|
| Visibilité des adresses de réseau privé | L'agent CylanceOPTICS enregistre les connexions réseau comprises dans les espaces d'adresse RFC 1918 et RFC 4193.<br>Ratio signal/bruit : Faible<br>Impact potentiel sur la conservation des données et les performances : Faible | Recommandé pour les ordinateurs de bureau.<br>Déconseillé pour :<br>• Serveurs DNS<br>• Systèmes avec peu ou sans ressources<br>• Systèmes qui utilisent RDP ou un autre logiciel d'accès à distance | • Ce capteur collecte une quantité importante de données et peut avoir un impact sur la durée pendant laquelle les données sont stockées dans la base de données CylanceOPTICS.<br>• BlackBerry recommande d'activer ce capteur uniquement dans les environnements dans lesquelles une visibilité complète de la communication d'adresse de réseau privé est requise. |
| Visibilité avancée de l'audit sous Windows | L'agent CylanceOPTICS surveille les types et catégories d'événements Windows supplémentaires.<br>Ratio signal/bruit : Modéré<br>Impact potentiel sur la conservation des données et les performances : Faible | — | Ce capteur permet de surveiller les ID d'événement suivants :<br>• 4769 - demande de ticket kerberos<br>• 4662 - opération sur un objet active directory<br>• 4624 connexion réussie<br>• 4702 création de tâches planifiées |
| Visibilité du journal des événements Windows | L'agent CylanceOPTICS enregistre les événements de sécurité Windows et leurs attributs associés.<br>Ratio signal/bruit : Modéré<br>Impact potentiel sur la conservation des données et les performances : Modéré | Recommandé pour :<br>• Ordinateurs de bureau<br>• Ordinateurs portables<br>• Serveurs<br>Déconseillé pour :<br>• Contrôleurs de domaine<br>• Microsoft Exchange et serveurs de messagerie | • Les journaux d'événements Windows à partir desquels ce capteur collecte des données sont fréquemment générés lors d'une utilisation normale du système.<br>• Pour réduire les doublons et améliorer la conservation des données, déterminez si votre organisation dispose déjà d'outils de collecte des données à partir des journaux d'événements Windows. |

### Structures de données utilisées par CylanceOPTICS pour identifier les menaces

Les évènements, artefacts et facets sont les trois principales structures de données utilisées par CylanceOPTICS pour analyser, enregistrer et examiner les activités qui se produisent sur les terminaux. Les fonctionnalités CylanceOPTICS s'appuient sur ces structures de données, y compris les requêtes InstaQuery, les données détaillés et le moteur d'analyse de contexte (CAE).

Cette section fournit plus d'informations sur la manière dont CylanceOPTICS interprète et interagit avec les activités sur les terminaux, afin de vous aider à mieux comprendre et utiliser les détections, les requêtes et les données détaillées.

#### Sources de données en fonction du système d'exploitation

L'agent CylanceOPTICS utilise les sources de données suivantes :

| OS | Sources de données |
|---|---|
| Windows | • Pilote de noyau CyOpticsDrv<br>• Suivi des évènements<br>• Fichier journal d'audit de sécurité |
| macOS | Pilote de noyau CyOpticsDrvOSX |
| Linux | ZeroMQ |

Pour plus d'informations sur les types de trafic réseau que CylanceOPTICS exclut par défaut, reportez-vous à l'article KB65604.

#### Évènements

Les évènements sont les composants qui entraînent une modification ou une action observable sur un terminal. Les évènements comportent deux artefacts principaux : l'artefact instigateur qui déclenche une action et l'artefact cible sur lequel des mesures sont prises.

Les tableaux suivants fournissent des détails sur les types d'évènements pouvant être détectés par CylanceOPTICS et avec lesquels il peut interagir.

**Évènement : indifférent**

- Option de stratégie de terminal à activer : case à cocher CylanceOPTICS
- Type d'artefact : processus, utilisateur
- Plateforme : Windows, macOS, Linux

| Type d'évènement | Description |
|---|---|
| Indifférent | Tous les évènements enregistrent le processus qui les a générés et l'utilisateur associé à l'action. |

**Évènement : application**

- Option de stratégie de terminal à activer : Visibilité WMI avancée
- Type d'artefact : suivi WMI
- Plateforme : Windows

| Type d'évènement | Description |
|---|---|
| Créer une liaison filtre-client | Un processus a utilisé la persistance WMI. |

| Type d'évènement | Description |
|---|---|
| Créer un client temporaire | Un processus s'est abonné aux évènements WMI. |
| Exécuter l'opération | Un processus a effectué une opération WMI. |

- Option de stratégie de terminal à activer : Visibilité améliorée des accrochages et des processus
- Type d'artefact : fichier
- Plateforme : Windows

| Type d'évènement | Description |
|---|---|
| CBT | L'API SetWindowsHookEx a installé un crochet pour recevoir des notifications utiles à une application CBT. |
| DebugProc | L'API SetWindowsHookEx a installé un crochet pour déboguer d'autres procédures de crochet. |
| Obtenir l'état de clé asynchrone | Un processus a appelé l'API Win32 GetAsyncKeyState. |
| JournalPlayback | L'API SetWindowsHookEx a installé un crochet pour surveiller les messages précédemment enregistrés par une procédure de crochet WH_JOURNALLECORD. |
| JournalRecord | L'API SetWindowsHookEx a installé un crochet pour surveiller les messages d'entrée publiés dans la file d'attente des messages système. |
| Clavier | L'API SetWindowsHookEx a installé un crochet pour surveiller les messages de frappe. |
| Clavier de bas niveau | L'API SetWindowsHookEx a installé un crochet pour surveiller les évènements de saisie clavier de bas niveau. |
| Souris de bas niveau | L'API SetWindowsHookEx a installé un crochet pour surveiller les évènements d'entrée de souris de bas niveau. |
| Message | L'API SetWindowsHookEx a installé un crochet pour surveiller les messages publiés dans une file d'attente de messages. |
| Souris | L'API SetWindowsHookEx a installé un crochet pour surveiller les messages de la souris. |
| Enregistrer les terminaux d'entrée brute | Un processus a appelé API Win32 RegisterRawInputDevices. |
| Définir le crochet d'événement Windows | Un processus a appelé l'API Win32 SetWinEventHook. |
| Configurer le crochet Windows | L'API SetWindowsHookEx a installé une valeur de type de crochet non répertoriée. |

| Type d'évènement | Description |
| --- | --- |
| ShellProc | L'API SetWindowsHookEx a installé un crochet pour recevoir des notifications utiles pour les applications de shell. |
| SysMsg | L'API SetWindowsHookEx a installé un crochet pour surveiller les messages générés à la suite d'un évènement d'entrée dans une boîte de dialogue, une boîte de message ou une barre de défilement. |
| WindowProc | L'API SetWindowsHookEx a installé un crochet pour surveiller les messages de procédure Windows. |

- Option de stratégie de terminal à activer : Détecteur API
- Type d'artefact : Appel API
- Plateforme : Windows

| Type d'évènement | Description |
| --- | --- |
| Fonction | Un appel de fonction remarquable a été effectué. |

- Option de stratégie de terminal à activer : Visibilité charge de module
- Type d'artefact : fichier
- Plateforme : Windows

| Type d'évènement | Description |
| --- | --- |
| Charger | Une application a chargé un module. |

- Option de stratégie de terminal à activer : Visibilité objet COM
- Plateforme : Windows

| Type d'évènement | Description |
| --- | --- |
| Créé | Un objet COM a été créé. |

**Évènement : terminal**

- Option de stratégie de terminal à activer : case à cocher CylanceOPTICS
- Type d'artefact : fichier
- Plateforme : macOS, Linux

| Type d'évènement | Description |
| --- | --- |
| Monter | Le terminal est connecté à une machine ou les dossiers sont montés sur des emplacements réseau spécifiques. |

**Évènement : fichier**

- Option de stratégie de terminal à activer : case à cocher CylanceOPTICS
- Type d'artefact : fichier

- Plateforme : Windows, macOS, Linux

| Type d'évènement | Description |
|---|---|
| Créer | Un fichier a été créé. |
| Supprimer | Un fichier a été supprimé. |
| Écraser | Un fichier a été écrasé. |
| Renommer | Un fichier a été renommé. |
| Écrire | Un fichier a été modifié. |

- Option de stratégie de terminal à activer : Visibilité améliorée de lecture de fichier
- Type d'artefact : fichier
- Plateforme : Windows

| Type d'évènement | Description |
|---|---|
| Ouvrir | Un fichier a été ouvert. |

**Évènement : mémoire**

- Option de stratégie de terminal à activer : case à cocher CylanceOPTICS
- Type d'artefact : processus
- Plateforme : macOS, Linux

| Type d'évènement | Description |
|---|---|
| Mmap | Une région de mémoire a été mappée dans un but spécifique, généralement allouée à un processus. |
| MProtect | Les métadonnées ont été modifiées pour une région de mémoire, généralement pour modifier son état (par exemple, pour le rendre exécutable). |

**Évènement : réseau**

- Option de stratégie de terminal à activer : case à cocher CylanceOPTICS
- Type d'artefact : réseau
- Plateforme : Windows, macOS, Linux

| Type d'évènement | Description |
|---|---|
| Se connecter | Une connexion réseau a été établie. Par défaut, le trafic local n'est pas collecté. |

- Option de stratégie de terminal à activer : Visibilité des adresses réseau privées
- Type d'artefact : réseau
- Plateforme : Windows

| Type d'évènement | Description |
|---|---|
| Se connecter | Les évènements de connexion incluent le trafic local. |

- Option de stratégie de terminal à activer : Visibilité DNS
- Type d'artefact : requête DNS
- Plateforme : Windows, Linux

| Type d'évènement | Description |
|---|---|
| Demande | Un processus a effectué une requête DNS réseau qui n'était pas mise en cache. |
| Réponse | Un processus a reçu une réponse DNS. |

- Option de stratégie de terminal à activer : Visibilité HTTP
- Type d'artefact : HTTP
- Plateforme : Windows

| Type d'évènement | Description |
|---|---|
| Get | Windows a utilisé WinINet ou WinHTTP pour créer une requête HTTP. |
| Post | Windows a utilisé WinINet ou WinHTTP pour envoyer des données. |

**Évènement : processus**

- Option de stratégie de terminal à activer : case à cocher CylanceOPTICS
- Type d'artefact : processus

| Type d'évènement | Plateforme | Description |
|---|---|---|
| Sortie anormale | macOS<br>Linux | Surveillé par le capteur de présélection, un processus s'est arrêté sans être terminé (par exemple, une exception a provoqué la fermeture d'un processus). |
| Quitter | Windows<br>macOS<br>Linux | Un processus a été arrêté. |
| Sortie forcée | macOS<br>Linux | Surveillé par le capteur de présélection, un processus a été forcé de quitter le système par un autre processus. |
| PTrace | macOS<br>Linux | Il s'agit d'un outil système Unix qui permet à un processus de surveiller et de contrôler un autre processus. |
| Démarrer | Windows<br>macOS<br>Linux | Un processus a démarré. |

| Type d'évènement | Plateforme | Description |
|---|---|---|
| Suspendre | Linux | Surveillé par le capteur de présélection, un processus a été suspendu. |
| Évènement de processus Linux inconnu | macOS<br>Linux | Surveillé par le capteur de présélection, un évènement inconnu s'est produit avec le processus comme cible. Cela peut indiquer qu'un logiciel malveillant masque son activité. |

- Option de stratégie de terminal à activer : Visibilité améliorée des accrochages et des processus
- Type d'artefact : processus
- Plateforme : Windows

| Type d'évènement | Description |
|---|---|
| SetThreadContext | Un processus a appelé l'API SetThreadContext. |
| Terminer | Un processus instigateur a mis fin à un autre processus cible. |

**Évènement : registre**

- Option de stratégie de terminal à activer : case à cocher CylanceOPTICS
- Type d'artefact : registre, fichier (si la clé de registre fait référence à un fichier spécifique)
- Plateforme : Windows

| Type d'évènement | Description |
|---|---|
| KeyCreated | Une clé de registre a été créée. |
| KeyDeleting | Une clé de registre a été supprimée. |
| ValueChanging | La valeur de clé de registre a été modifiée. |
| ValueDeleting | Une valeur de clé de registre a été supprimée. |

**Évènement : scripts**

- Option de stratégie de terminal à activer : Visibilité avancée des scripts
- Type d'artefact : suivi PowerShell
- Plateforme : Windows

| Type d'évènement | Description |
|---|---|
| Exécuter la commande | Windows PowerShell a exécuté une commande. Les paramètres sont inconnus. |
| Exécuter le script | Windows PowerShell a exécuté un script. |
| Exécuter le bloc de script | Windows PowerShell a exécuté un bloc de script. |

| Type d'évènement | Description |
|---|---|
| Appeler la commande | Windows PowerShell a appelé une commande avec des paramètres liés. |
| Empêcher le script | Un résultat de ScanBuffer AMSI indique qu'un script a été détecté ou bloqué par un administrateur. |

**Évènement : utilisateur**

- Option de stratégie de terminal à activer : Visibilité avancée des scripts
- Type d'artefact : événement Windows
- Plateforme : Windows

| Type d'évènement | Description |
|---|---|
| Déconnexion du lot | L'ID d'évènement Windows suivant s'est produit : 4634 (type 4). |
| Connexion au lot | L'ID d'évènement Windows suivant s'est produit : 4624 (type 4). |
| Déconnexion interactive en cache | L'ID d'évènement Windows suivant s'est produit : 4634 (type 11). |
| Connexion interactive en cache | L'ID d'évènement Windows suivant s'est produit : 4624 (type 11). |
| Déconnexion interactive | L'ID d'évènement Windows suivant s'est produit : 4634 (type 2). |
| Connexion interactive | L'ID d'évènement Windows suivant s'est produit : 4624 (type 2). |
| Déconnexion du réseau | L'ID d'évènement Windows suivant s'est produit : 4634 (type 3). |
| Connexion réseau | L'ID d'évènement Windows suivant s'est produit : 4624 (type 3). |
| Déconnexion au réseau en texte clair | L'ID d'évènement Windows suivant s'est produit : 4634 (type 8). |
| Connexion au réseau en texte clair | L'ID d'évènement Windows suivant s'est produit : 4624 (type 8). |
| Déconnexion des nouveaux identifiants | L'ID d'évènement Windows suivant s'est produit : 4634 (type 9). |

| Type d'évènement | Description |
|---|---|
| Connexion aux nouveaux identifiants | L'ID d'évènement Windows suivant s'est produit : 4624 (type 9). |
| Déconnexion interactive à distance | L'ID d'évènement Windows suivant s'est produit : 4634 (type 10). |
| Connexion interactive à distance | L'ID d'évènement Windows suivant s'est produit : 4624 (type 10). |
| Déconnexion du service | L'ID d'évènement Windows suivant s'est produit : 4634 (type 5). |
| Connexion au service | L'ID d'évènement Windows suivant s'est produit : 4624 (type 5). |
| Déverrouiller la déconnexion | L'ID d'évènement Windows suivant s'est produit : 4634 (type 7). |
| Déverrouiller la connexion | L'ID d'évènement Windows suivant s'est produit : 4624 (type 7). |
| Déconnexion utilisateur | L'ID d'évènement Windows suivant s'est produit : 4634 (valeur de type non répertoriée). |
| Connexion utilisateur | L'ID d'évènement Windows suivant s'est produit : 4624 (valeur de type non répertoriée). |

#### Artefacts et facets

Les artefacts sont des éléments d'information complexes pouvant être utilisés par CylanceOPTICS. Le moteur d'analyse de contexte (CAE) peut identifier les artefacts sur les terminaux et les utiliser pour déclencher une réponse automatique aux incidents et des actions correctives. Les requêtes InstaQueries utilisent des artefacts comme base d'une requête.

Les facets sont les attributs d'un artefact qui peuvent être utilisés pour identifier les traits d'un artefact associé à un évènement. Les facets sont corrélés et combinés pendant l'analyse pour identifier les activités potentiellement malveillantes. Par exemple, un fichier nommé « explorer.exe » peut ne pas être intrinsèquement suspect, mais si le fichier n'est pas signé par Microsoft et qu'il réside dans un répertoire temporaire, il peut être identifié comme suspect dans certains environnements.

CylanceOPTICS utilise les artefacts et facets suivants :

| Artefact | Facets |
|---|---|
| Appel d'API | • Fonction<br>• DLL<br>• Paramètres |

| Artefact | Facets |
|---|---|
| DNS | • Connexion<br>• IsRecursionDesired<br>• IsUnsolicitedResponse<br>• Opcode<br>• RequestId<br>• Résolution<br>• ResponseOriginatedFromThisDevice<br>• Questions |
| Évènement | • Heure d'occurrence<br>• Heure d'enregistrement |
| Fichier | • Enregistrement de fichier exécutable (fichiers binaires uniquement)<br>• Heure de création du fichier (signalée par le système d'exploitation)<br>• Chemin du fichier<br>• Signature de fichier (fichiers binaires uniquement)<br>• Taille du fichier<br>• Heure de la dernière modification (signalée par le système d'exploitation)<br>• Hachage md5 (fichiers binaires uniquement)<br>• Emplacement d'écriture récent<br>• Hachage sha256 (fichiers binaires uniquement)<br>• Type de fichier suspecté<br>• Utilisateur |
| Réseau | • Adresse locale<br>• Port local<br>• Protocole<br>• Adresse distante<br>• Port distant |
| Suivi PowerShell | • EventId<br>• Charge utile<br>• PayloadAnalysis<br>• ScriptBlockText<br>• ScriptBlockTextAnalysis |
| Processus | • Ligne de commande<br>• Fichier à partir duquel l'exécutable a été exécuté<br>• Processus parent<br>• ID de processus<br>• Heure de début<br>• Utilisateur |
| Registre | • Si la valeur fait référence à un fichier sur le système<br>• Chemin de registre<br>• Valeur |

| Artefact | Facets |
| --- | --- |
| Utilisateurs | • Domaine<br>• Identifiant spécifique au système d'exploitation (par exemple, SID)<br>• Nom d'utilisateur<br><br>Les artefacts utilisateur peuvent contenir l'une des valeurs suivantes. Cependant, les données ne sont pas disponibles sur la plupart des terminaux.<br><br>• AccountType<br>• BadPasswordCount<br>• Commentaire<br>• CountryCode<br>• FullName<br>• HasPasswordExpired<br>• HomeDirectory<br>• IsAccountDisabled<br>• IsLocalAccount<br>• IsLockedOut<br>• IsPasswordRequired<br>• LanguageCodePage<br>• LogonServer<br>• PasswordAge<br>• PasswordDoesNotExpire<br>• ProfilePath<br>• ScriptPath<br>• UserPrivilege<br>• Workstations |
| Évènement Windows | • Classe<br>• ID d'évènement<br>• Serveur objet<br>• Liste de privilèges<br>• ID de processus<br>• Nom du processus<br>• Nom du fournisseur<br>• Service<br>• Nom du domaine objet<br>• ID de connexion objet<br>• Nom d'utilisateur objet<br>• Sid d'utilisateur objet |
| Suivi WMI | • ConsumerText<br>• ConsumerTextAnalysis<br>• EventId<br>• Espace de noms<br>• Opération<br>• OperationAnalysis<br>• OriginatingMachineName |

#### Valeurs et clés de registre

CylanceOPTICS surveille les valeurs et les clés communes de persistance, de démarrage de processus et d'escalade des privilèges, ainsi que les valeurs indiquées dans l'article KB 66266.

Pour en savoir plus sur la manière dont CylanceOPTICS surveille les points de persistance dans le registre, consultez l'article KB 66357.

# Configurer CylanceGATEWAY

**Remarque :** Si CylanceGATEWAY n'est pas activé pour votre locataire, les options de menu permettant de le configurer ne s'affichent pas dans la console de gestion. Si un utilisateur avec des autorisations insuffisantes se connecte à la console de gestion, un message d'erreur aucune autorisation s'affiche lors de la sélection d'une option de menu. Pour plus d'informations sur le message d'erreur, rendez-vous sur support.blackberry.com/community pour consulter l'article 98223.

La résolution DNS des adresses IPv6 n'est pas prise en charge. Les adresses IPv6 ne seront pas renvoyées à l'agent CylanceGATEWAY.

| Étape | Action |
|---|---|
| 1 | Installez et configurez le BlackBerry Connectivity Node et au moins un CylanceGATEWAY Connector. |
| 2 | Spécifiez les adresses faisant partie de votre réseau privé. |
| 3 | Spécifiez vos paramètres DNS privés et vos suffixes. |
| 4 | Passez en revue les services réseau CylanceGATEWAY existants ou définissez les vôtres pour faciliter la création de règles de liste de contrôle d'accès (ACL) sur les locataires (facultatif). |
| 5 | Configurez des règles ACL sur les locataires pour gérer les destinations Internet et de réseau privé qui autorisent et bloquent l'accès à CylanceGATEWAY. |
| 6 | Configurer la protection réseau Spécifiez les menaces détectées par CylanceGATEWAY et la manière dont elles réagissent. |
| 7 | Ajoutez des utilisateurs pour CylanceGATEWAY. |
| 8 | Configurer les options des services Gateway Spécifiez des options spécifiques au système d'exploitation. |
| 9 | Configurez les stratégies d'inscription pour permettre aux utilisateurs d'activer l'application CylancePROTECT Mobile ou l'agent CylanceGATEWAY sur leurs terminaux. |
| 10 | Attribuer des stratégies à des administrateurs, des utilisateurs et des groupes. Les utilisateurs doivent se voir attribuer une stratégie d'inscription et une stratégie de service Gateway avant de pouvoir activer l'agent CylanceGATEWAY. |

| Étape | Action |
| --- | --- |
| 11 | Les utilisateurs de terminaux installent et activent l'application CylancePROTECT Mobile sur iOS, Android les terminaux Chromebook et l'agent CylanceGATEWAY sur les terminaux Windows et macOS. Vous pouvez éventuellement effectuer une installation ou une mise à niveau en mode silencieux de l'agent CylanceGATEWAY.<br><br>Vous pouvez télécharger les agents depuis le site Web de BlackBerry. Pour plus d'informations sur l'application CylancePROTECT Mobile et l'agent CylanceGATEWAY, reportez-vous au Guide de l'utilisateur Cylance Endpoint Security.<br><br>Vous pouvez également intégrer Cylance Endpoint Security à BlackBerry UEM ou Microsoft Intune pour vérifier si les terminaux iOS et Android sont gérés par UEM ou Intune avant de pouvoir utiliser CylanceGATEWAY. Pour plus d'informations, reportez-vous à Connexion de Cylance Endpoint Security aux solutions MDM pour vérifier si les terminaux sont gérés. |
| 12 | Apporter vos propres adresses IP (BYOIP) pour fournir des adresses IP dédiées plus grandes pour contrôler le trafic de différentes manières, par exemple en utilisant l'adresse IP de votre entreprise pour rechercher l'épinglage d'adresses IP et en autorisant une seule plage d'adresses IP ou une adresse CIDR au lieu de plusieurs adresses IP non continues. (Facultatif) |

# Définition de votre réseau privé

Pour utiliser CylanceGATEWAY en vue de contrôler l'accès à vos réseaux privés, vous devez définir vos réseaux privés. Lorsque vous définissez vos réseaux privés, vous pouvez configurer CylanceGATEWAY pour appliquer le privilège et la microsegmentation les plus restrictifs lorsque les utilisateurs accèdent à vos ressources réseau. CylanceGATEWAY prend en charge l'accès à plusieurs réseaux privés (par exemple, segments, centres de données et VPC) dans les environnements sur site et dans le cloud. CylanceGATEWAY empêche les utilisateurs de se connecter à n'importe quel emplacement de votre réseau privé, sauf si une règle de liste de contrôle d'accès (ACL) autorisant la connexion lui est attribuée.

Vous pouvez définir vos réseaux privés en ajoutant un groupe de connecteurs pour chaque réseau privé sur lequel vous souhaitez que les utilisateurs puissent accéder aux ressources. Si votre service CylanceGATEWAY a été activé avant juillet 2023 et qu'il comprenait un ou plusieurs CylanceGATEWAY Connectors, tous vos connecteurs existants ont été déplacés vers le « Groupe de connecteurs par défaut ». Vous pouvez renommer le groupe de connecteurs par défaut ou ajouter des groupes supplémentaires et attribuer les connecteurs selon vos besoins.

Chaque locataire prend en charge un maximum de huit groupes de connecteurs.

Les groupes de connecteurs sont les suivants :

- Adresses IP, plages d'adresses IP et notation CIDR que vous spécifiez pour chaque groupe. CylanceGATEWAY Connectors reconnaissent ces adresses comme faisant partie de l'un de vos réseaux privés.
- L'URL de contrôle d'intégrité. Propre au groupe, elle est utilisée par chaque membre CylanceGATEWAY Connector du groupe pour confirmer la connectivité à votre réseau privé.
- Les restrictions IP que vous pouvez définir de façon à ce que Gateway accepte les connexions uniquement à partir des connecteurs sur les adresses IP spécifiées.

Pour établir un tunnel sécurisé entre les terminaux des utilisateurs et vos réseaux privés, vous devez installer un ou plusieurs CylanceGATEWAY Connectors.

Chaque groupe de connecteurs prend en charge un maximum de huit CylanceGATEWAY Connectors.

Vous pouvez également spécifier les adresses de vos serveurs DNS privés et les suffixes DNS privés utilisés pour les recherches. Les paramètres DNS s'appliquent à tous les connecteurs de groupe de votre environnement et doivent être ajoutés à un groupe.

Dans les environnements qui contiennent plusieurs groupes avec des adresses IP de destination ou des plages d'adresses IP similaires, le flux de données est dirigé, dans l'ordre, vers les groupes de connecteurs répertoriés jusqu'à ce que l'adresse IP soit mise en correspondance avec un groupe de connecteurs. Le groupe de connecteurs qui inclut l'adresse IP mise en correspondance est ensuite utilisé pour acheminer la connexion vers la destination afin d'accéder aux ressources.

## Installation du connecteur CylanceGATEWAY

Le système CylanceGATEWAY Connector est une appliance virtuelle que vous devez installer si vous souhaitez utiliser CylanceGATEWAY pour établir un tunnel sécurisé entre les terminaux des utilisateurs et vos réseaux privés. Le CylanceGATEWAY Connector doit être déployé et inscrit dans une partie du réseau qui dispose d'un accès complet aux adresses que vous définissez lorsque vous Spécifier votre réseau privé. Si vous n'installez pas de CylanceGATEWAY Connector, vous pouvez utiliser CylanceGATEWAY uniquement pour bloquer l'accès aux destinations Internet publiques et sécuriser l'accès aux applications cloud à l'aide de l'épinglage IP source.

Il est recommandé d'installer plus d'un CylanceGATEWAY Connector. Installer plusieurs instances permet d'équilibrer la charge pour accéder à des segments distincts ou à des clouds privés au sein de votre Définition de votre réseau privé. Lorsque plusieurs instances du CylanceGATEWAY Connector sont installées et configurées sur votre réseau, les connexions des clients sont réparties uniformément sur tous les terminaux CylanceGATEWAY Connector intègres affectés au même groupe de connecteurs, fournissant ainsi une redondance dans le cas où une instance deviendrait indisponible ou lors de la résolution de problèmes.

Chaque locataire prend en charge un maximum de huit groupes de connecteurs.

Chaque groupe de connecteurs prend en charge un maximum de huit CylanceGATEWAY Connectors.

BlackBerry vous recommande de spécifier une URL de contrôle d'intégrité dans chaque groupe de connecteurs pour surveiller régulièrement l'état de chaque CylanceGATEWAY Connector. Si vous ne spécifiez pas d'URL de contrôle d'intégrité, CylanceGATEWAY ne peut pas confirmer si vous disposez d'une connectivité à votre réseau privé, et la colonne État du contrôle d'intégrité (Réseau privé > Connecteurs Gateway) d'un connecteur n'affiche pas les informations DNS et HTTP. Pour plus d'informations, reportez-vous à Gestion des connecteurs CylanceGATEWAY.

Contactez votre représentant commercial BlackBerry si vous prévoyez d'installer CylanceGATEWAY dans un environnement qui nécessite un package différent.

Pour configurer un CylanceGATEWAY Connector, effectuez les opérations suivantes.

| Étape | Action |
| --- | --- |
| 1 | Examinez Configuration requise : connecteur CylanceGATEWAY. |

| Étape | Action |
|---|---|
| 2 | Installer le CylanceGATEWAY Connector dans votre environnement Le CylanceGATEWAY Connector est pris en charge dans les environnements suivants. Pour obtenir des instructions détaillées sur l'installation de CylanceGATEWAY Connector dans votre environnement, consultez la section Installer le flux de travail CylanceGATEWAY Connector pour votre environnement.<br>• Environnement vSphere<br>• Environnement ESXi<br>• Environnement Microsoft Entra ID<br>• Environnement Hyper-V<br>• Environnement AWS |
| 3 | Configurer le CylanceGATEWAY Connector dans l'environnement de la machine virtuelle (facultatif). |
| 4 | Accéder au CylanceGATEWAY Connector à l'aide d'OpenSSH (facultatif). |
| 5 | Configurer votre pare-feu pour CylanceGATEWAY Connector. |
| 6 | Inscrivez le CylanceGATEWAY Connector auprès de BlackBerry Infrastructure. |
| 7 | Configurer le CylanceGATEWAY Connector (facultatif). |
| 8 | Gestion de CylanceGATEWAY Connectors pour définir les options et vérifier l'état du connecteur. |

#### Installer le connecteur CylanceGATEWAY dans un environnement vSphere

Vous pouvez configurer le CylanceGATEWAY Connector avec une IP statique. Si vous souhaitez apporter des modifications à la configuration réseau du CylanceGATEWAY Connector après son installation, vous pouvez modifier les options vApp de la machine virtuelle et redémarrer le CylanceGATEWAY Connector pour que les modifications prennent effet. Pour savoir comment modifier les détails OVF, consultez la documentation VMware intitulée « Modifier les détails OVF pour une machine virtuelle »).

**Avant de commencer :** Assurez-vous que vous disposez des autorisations nécessaires pour déployer un modèle OVF dans un environnement vSphere.

1. Téléchargez le fichier OVA du CylanceGATEWAY Connector (cylance-gateway-connector-<*version*>.ova) à partir de *my*Account.
2. Connectez-vous à l'environnement vSphere.
3. Cliquez avec le bouton droit de la souris sur le cluster sur lequel vous souhaitez installer le CylanceGATEWAY Connector et sélectionnez **Déployer le modèle OVF**.
4. Sur l'écran **Sélectionner un modèle OVF**, cliquez sur **Fichier local**.
5. Cliquez sur **Charger des fichiers** et accédez au fichier cylance-gateway-connector.ova.

6. Cliquez sur **Suivant**.
7. Sur l'écran **Sélectionner un nom et un dossier**, saisissez un nom pour la machine virtuelle, puis cliquez sur **Suivant**.

   Le nom par défaut est cylance-gateway-connector.
8. Sur l'écran **Sélectionner une ressource d'ordinateur**, sélectionnez un emplacement pour la machine virtuelle, puis cliquez sur **Suivant**.
9. Une fois les vérifications de compatibilité terminées, cliquez sur **Suivant**.
10. Sur l'écran **Examiner les détails**, vérifiez les informations de configuration et cliquez sur **Suivant**.
11. Sur l'écran **Sélectionner le stockage**, pour **Format de disque virtuel**, sélectionnez **Provisionnement dynamique** et cliquez sur **Suivant**.
12. Sur l'écran **Sélectionner des réseaux**, configurez le **réseau de destination** pour ce CylanceGATEWAY Connector.

    Définissez le **réseau source** sur NAT.
13. Cliquez sur **Suivant**.
14. Sur l'écran **Personnaliser le modèle**, spécifiez des propriétés supplémentaires de machine virtuelle (facultatif).

    **Remarque :** Les adresses IP doivent être saisies sous la forme d'adresses IPv4 en notation décimale à points.

    - Par défaut, l'option **Utiliser le DHCP** est activée et le connecteur utilise des adresses IP automatiquement attribuées. Si vous souhaitez configurer le connecteur avec une adresse IP statique, vous devez décocher la case Utiliser le DHCP et fournir les adresses IP pour les paramètres suivants :
    - Dans le champ **Adresse IP/Longueur du préfixe**, saisissez l'adresse IP et le préfixe qui peuvent être attribués aux terminaux (par exemple, 192.0.2.100/24). Si vous ajoutez plusieurs adresses IP, séparez chaque adresse IP et préfixe par une virgule (,).
    - Dans le champ **Passerelle**, saisissez l'adresse IP de la passerelle réseau (par exemple, 192.0.2.1).
    - Dans le champ **DNS**, spécifiez l'adresse IP des serveurs DNS que vous souhaitez utiliser (par exemple, 192.0.2.120). Si vous ajoutez plusieurs serveurs DNS, séparez les adresses par une virgule (,).
15. Sur l'écran **Prêt pour la finalisation**, vérifiez les paramètres de configuration et cliquez sur **Terminer**.

**À la fin :** Après avoir installé le connecteur, vous pouvez vérifier que le fichier OVA est correctement installé dans l'environnement virtuel. Pour obtenir des instructions, reportez-vous à Configurer le CylanceGATEWAY Connector dans l'environnement de la machine virtuelle.

#### Installer CylanceGATEWAY Connector dans un environnement ESXi

Vous pouvez configurer l'interface réseau du CylanceGATEWAY Connector pour utiliser le DHCP ou configurer une adresse IP statique uniquement lorsque vous installez le CylanceGATEWAY Connector. Si vous souhaitez apporter des modifications à la configuration, vous devez désinstaller, puis installer le CylanceGATEWAY Connector avec la nouvelle configuration d'interface réseau.

**Avant de commencer :** Assurez-vous que vous disposez des autorisations nécessaires pour déployer un modèle OVF dans un environnement ESXi.

1. Téléchargez le fichier OVA du CylanceGATEWAY Connector (cylance-gateway-connector-<*version*>.ova) à partir de *my*Account.
2. Connectez-vous à l'environnement ESXi.
3. Dans le volet **Navigator** (Navigateur), sélectionnez **Virtual Machines** (Machines virtuelles).
4. Cliquez sur le bouton **Create/Register VM** (Créer/Inscrire une machine virtuelle).
5. Sur l'écran **New Virtual Machine** (Nouvelle machine virtuelle), sélectionnez **Deploy a Virtual machine from an OVF or OVA file** (Déployer une machine virtuelle à partir d'un fichier OVF ou OVA), puis cliquez sur **Next** (Suivant).
6. Saisissez le nom de la machine virtuelle.

7. Accédez au fichier cylance-gateway-connector-<*version*>.ova. Faites glisser le fichier et déposez-le dans la boîte de dialogue.
8. Cliquez sur **Suivant**.
9. Sur l'écran **Select storage** (Sélectionner le stockage), sélectionnez **Standard** et une banque de données, puis cliquez sur **Next** (Suivant).
10. Sur l'écran **Deployment options** (Options de déploiement), pour **Disk provisioning** (Approvisionnement du disque), sélectionnez **Thin** (Fin).
11. Sur l'écran **Paramètres supplémentaires**, développez Options pour spécifier des propriétés VMware supplémentaires (facultatif).

    **Remarque :** Les adresses IP doivent être saisies sous la forme d'adresses IPv4 en notation décimale à points.

    - Par défaut, l'option **Utiliser le DHCP** est activée et le connecteur utilise des adresses IP automatiquement attribuées. Si vous souhaitez configurer le connecteur avec une adresse IP statique, vous devez décocher la case Utiliser le DHCP et fournir les adresses IP pour les paramètres suivants :
    - Dans le champ **Adresse IP/Longueur du préfixe**, saisissez l'adresse IP et le préfixe qui peuvent être attribués aux terminaux (par exemple, 192.0.2.100/24). Pour utiliser plusieurs adresses IP, séparez les adresses IP par une virgule (,).
    - Dans le champ **Passerelle**, saisissez l'adresse de la passerelle réseau (par exemple, 192.0.2.1)
    - Dans le champ **DNS**, spécifiez l'adresse IP des serveurs DNS que vous souhaitez utiliser (par exemple, 192.0.2.120). Pour utiliser plusieurs serveurs DNS, séparez les adresses par une virgule (,).
12. Cliquez sur **Suivant**.
13. Sur l'écran **Prêt pour la finalisation**, vérifiez les paramètres de configuration et cliquez sur **Terminer**.

**À la fin :** Après avoir installé le connecteur, vous pouvez vérifier que le fichier OVA est correctement installé dans l'environnement virtuel. Pour obtenir des instructions, reportez-vous à Configurer le CylanceGATEWAY Connector dans l'environnement de la machine virtuelle.

#### Conditions préalables à l'installation du CylanceGATEWAY Connector dans un environnement Microsoft Entra ID

- Assurez-vous que le DNS est activé sur votre réseau privé Entra et qu'il est accessible par la machine virtuelle du connecteur.
- Vous pouvez également vérifier que votre environnement de réseau privé dispose d'un serveur proxy pour le trafic HTTP et HTTPS sortant.
- Veillez à ce que les services que vous souhaitez mettre à disposition via CylanceGATEWAY soient accessibles par le CylanceGATEWAY Connector sur votre réseau privé.
- Assurez-vous de pouvoir déployer un modèle VHD dans un environnement Entra.

#### Installer le CylanceGATEWAY Connector dans un environnement Microsoft Entra ID

Lorsque vous installez le connecteur, vous téléchargez le fichier VHD en tant que blob sur le portail Microsoft Entra ID. Utilisez le blob pour créer une image utilisée par la machine virtuelle du connecteur. Pour plus d'informations sur la configuration de votre environnement Entra, consultez la documentation du portail Azure - Portail Azure | Microsoft Docs.

**Avant de commencer :** Examinez Conditions préalables à l'installation du CylanceGATEWAY Connector dans un environnement Microsoft Entra ID.

1. Téléchargez le fichier VHD CylanceGATEWAY Connector (cylance-gateway-connector-fixed-<*version*>.vhd) depuis *my*Account.
2. Connectez-vous au portail de gestion Microsoft Entra ID à l'adresse suivante : https://portal.azure.com.
3. Téléchargez le fichier VHD en tant que blob.

a) Dans la section **Services Azure**, cliquez sur **Comptes de stockage**. Si vous ne disposez pas d'un compte de stockage, vous pouvez en créer un.
b) Cliquez sur votre compte de stockage.
c) Dans la colonne de gauche, dans la section **Stockage des données**, cliquez sur **Conteneurs**. Si vous ne disposez pas d'un conteneur, vous pouvez en créer un.
d) Sélectionnez votre conteneur.
e) Cliquez sur **Télécharger**.
f) Dans l'écran **Télécharger le blob**, accédez au fichier cylance-gateway-connector-fixed-<*version*>.vhd téléchargé.
g) Développez **Avancé** et définissez **Blob de page** dans la liste déroulante **Type de blob**.
h) Cliquez sur **Télécharger**.

**4.** Créez une image à partir du blob téléchargé.
a) Dans la colonne de gauche du portail de gestion, cliquez sur le menu du portail **> Tous les services**.
b) Dans le champ **Services de filtre**, saisissez `images`.
c) Cliquez sur **Images** et vérifiez que l'image utilise le type de ressource **Microsoft.Compute/images**.
d) Cliquez sur **Créer**.
e) Renseignez les champs requis pour votre environnement. Dans la section **Disque du système d'exploitation**, spécifiez les paramètres suivants :
   - Type de système d'exploitation : Linux
   - Génération de machine virtuelle : Gen 1
   - Blob de stockage : accédez au blob que vous avez créé à l'étape 3.
f) Cliquez sur l'onglet **Balises** et ajoutez des balises (facultatif).
g) Cliquez sur **Vérifier + créer**.
h) Cliquez sur **Créer**.
i) Cliquez sur **Accéder à la ressource**. L'écran Créer une machine virtuelle s'ouvre.

**5.** Créez une machine virtuelle de connecteur.
a) Dans l'onglet **Concepts de base**, renseignez les champs requis pour votre environnement. Spécifiez les paramètres suivants :
   - Image : sélectionnez l'image que vous avez créée à l'étape 4.
   - Taille : sélectionnez une taille comprenant 2 vCPU et au moins 4,5 Go de mémoire.
   - Type d'authentification : sélectionnez **Mot de passe**.
   - Nom d'utilisateur : saisissez une valeur. L'image de la machine virtuelle du connecteur ne tient pas compte de ce champ.
   - Mot de passe et Confirmer le mot de passe : saisissez une valeur. L'image de la machine virtuelle du connecteur ne tient pas compte de ces champs.
b) Cliquez sur l'onglet **Disques**.
c) Sur la page **Disques**, dans la liste déroulante **Type de disque du système d'exploitation**, sélectionnez **Disque dur standard**. La machine virtuelle du connecteur ne nécessite pas d'accéder au disque à faible latence.
d) Cliquez sur l'onglet **Mise en réseau**. Renseignez les champs requis pour votre environnement. Assurez-vous que l'image du connecteur utilise votre réseau privé. Le connecteur ne prend pas en charge la fonction de mise en réseau accélérée de Entra. Si vous activez ce paramètre, la machine virtuelle du connecteur risque de ne pas fonctionner comme prévu.
e) Cliquez sur l'onglet **Gestion**. L'image ne prend pas en charge la « connexion avec Azure AD ». Si vous activez ce paramètre, la machine virtuelle du connecteur risque de ne pas fonctionner comme prévu.
f) Cliquez sur l'onglet **Avancé**. Configurez selon les besoins de votre environnement. Le connecteur ne prend pas en charge les paramètres « Données personnalisées » ou « Données utilisateur ». Les paramètres « Données personnalisées » ou « Données utilisateur » peuvent être configurés selon les besoins de votre

environnement, mais ils ne sont pas pris en compte par la machine virtuelle du connecteur. BlackBerry déconseille l'installation d'applications de machine virtuelle supplémentaires sur la machine virtuelle qui exécute la machine virtuelle du connecteur.

g) Cliquez sur l'onglet **Balises**. Configurez les balises selon les besoins de votre environnement.
h) Cliquez sur l'onglet **Vérifier + créer**. Passez en revue votre configuration.
i) Cliquez sur **Créer**.

**Remarque :** Un message d'erreur de délai d'expiration peut s'afficher lors de la création de la ressource de machine virtuelle. Actualisez l'écran, le cas échéant.

#### Installer le CylanceGATEWAY Connector dans un environnement Hyper-V

**Avant de commencer :** Vérifiez que vous disposez des autorisations nécessaires pour déployer le fichier VHD et créez une image de connecteur.

1. Téléchargez le fichier VHD CylanceGATEWAY Connector (cylance-gateway-connector-dynamic<*version*>.vhd) depuis *my*Account.
2. Exécutez le gestionnaire Hyper-V en tant qu'administrateur.
3. Dans le menu du gestionnaire Hyper-V, cliquez sur **Action > Nouveau > Machine virtuelle**. Cliquez sur **Suivant**.
4. Sur l'écran **Spécifier un nom et un emplacement**, spécifiez un nom pour la machine virtuelle. Cliquez sur **Suivant**.
5. Sur l'écran **Spécifier la génération**, sélectionnez **Génération 1**. Cliquez sur **Suivant**.
6. Sur l'écran **Affecter la mémoire**, cliquez sur **Suivant**.
7. Sur l'écran **Configurer la mise en réseau**, sélectionnez la connexion appropriée. Cliquez sur **Suivant**.
8. Sur l'écran **Connecter un disque dur virtuel**, sélectionnez **Utiliser un disque dur virtuel existant**.
9. Accédez au fichier cylance-gateway-connector-dynamics-<*version*>.vhd que vous avez téléchargé à l'étape 1.
10. Sur l'écran **Attribuer de la mémoire**, assurez-vous que le connecteur dispose d'au moins 5 Go de mémoire. Cliquez sur **Suivant**.
11. Sur l'écran **Fin de l'Assistant Nouvel ordinateur virtuel**, vérifiez les paramètres de configuration, puis cliquez sur **Terminer**.
12. Démarrez le connecteur.

**À la fin :** Après avoir installé le connecteur, vous pouvez vérifier que le fichier VHD est correctement installé dans l'environnement virtuel. Pour obtenir des instructions, reportez-vous à Configurer le CylanceGATEWAY Connector dans l'environnement de la machine virtuelle.

#### Installer le CylanceGATEWAY Connector dans un environnement AWS

Vous installez CylanceGATEWAY Connector à l'aide de l'AMI dans Marketplace AWS.

1. Connectez-vous à la console de gestion AWS à l'adresse https://aws.amazon.com/console.
2. Pour créer l'instance de CylanceGATEWAY Connector. Procédez comme suit :
   a. Ouvrez le service **EC2**.
   b. Dans la colonne de gauche, sous **Instances**, cliquez sur **Instances**.
   c. Cliquez sur **Lancer les instances**.
   d. Sur l'écran **Lancer une instance**, saisissez un nom pour l'instance CylanceGATEWAY Connector.
   e. Dans la section **Amazon Machine Image (AMI)**, cliquez sur **Parcourir d'autres AMI**.
   f. Sur l'écran **Choisir une Amazon Machine Image (AMI)**, cliquez sur l'onglet **AMI AWS Marketplace**.
   g. Dans le champ de recherche **AMI sélectionnée**, saisissez `CylanceGATEWAY`. Appuyez sur la touche **Entrée**.
   h. Sélectionnez un type d'instance en fonction des exigences de votre organisation.

**Remarque :** BlackBerry recommande de sélectionner un type d'instance c6in ou c5n pour les environnements de production.

i. Sélectionnez une paire de clés pour vous connecter en toute sécurité à votre instance de connecteur via OpenSSH.
j. Dans la section **Paramètres réseau**, cliquez sur **Modifier** et spécifiez les paramètres suivants :
   1. Cliquez sur la liste déroulante **VPC** et sélectionnez votre réseau privé.
   2. Vous pouvez également cliquer sur **Attribuer automatiquement l'adresse IP publique** et sélectionner **Activer**. Vous devez attribuer une adresse IP publique au système CylanceGATEWAY Connector uniquement si vous n'avez pas le moyen d'accéder à l'interface Web du connecteur à l'aide du réseau privé sur lequel il est installé.
   3. Sélectionnez ou créez un groupe de sécurité en fonction des exigences de votre organisation. Le groupe de sécurité doit disposer d'un accès au port 22 (SSH), au port 80 (HTTP) et au port 443 (HTTPS) au CylanceGATEWAY Connector à partir du réseau sur lequel l'inscription est effectuée.
k. Cliquez sur **Lancer l'instance**.

**À la fin :** Inscrivez le CylanceGATEWAY Connector auprès de BlackBerry Infrastructure

#### Configurer le CylanceGATEWAY Connector dans l'environnement de la machine virtuelle

**Remarque :** L'AMI CylanceGATEWAY Connector AWS ne prend pas en charge l'accès à la console série EC2. N'effectuez pas cette tâche si vous installez le connecteur dans votre environnement AWS. Reportez-vous à la section Configurer votre pare-feu pour CylanceGATEWAY Connector pour poursuivre la configuration CylanceGATEWAY Connector.

Le CylanceGATEWAY Connector est une installation minimale du système d'exploitation Ubuntu, qui peut fonctionner sans connexion de l'utilisateur. Vous devez vous connecter uniquement si vous souhaitez mettre à jour les paramètres par défaut ou vérifier que l'OVA ou le VHD a été déployé correctement.

1. Effectuez l'une des opérations suivantes pour ouvrir la console dans votre environnement.

| Environnement | Étapes |
|---|---|
| vSphere | **a.** Connectez-vous à votre environnement.<br>**b.** Cliquez sur le nom d'hôte du CylanceGATEWAY Connector.<br>**c.** Cliquez sur **Lancer à distance** ou sur **Lancer la console Web**. |
| ESXi | **a.** Connectez-vous à votre environnement.<br>**b.** Cliquez sur le nom d'hôte du CylanceGATEWAY Connector.<br>**c.** Cliquez sur **Console**. |
| Microsoft Entra ID | **a.** Connectez-vous au portail de gestion Microsoft Entra ID à l'adresse https://portal.azure.com.<br>**b.** Cliquez sur **Machines virtuelles**.<br>**c.** Dans la colonne de gauche, dans la section **Support + dépannage**, cliquez sur **Console série**. |
| Hyper-V | **a.** Ouvrez le gestionnaire Hyper-V.<br>**b.** Cliquez avec le bouton droit de la souris sur le connecteur auquel vous souhaitez accéder **> Connecter**. |

2. À l'invite UNIX, saisissez le nom d'utilisateur de l'administrateur et appuyez sur **Entrée**.
   La valeur par défaut est **admin**.

3. Saisissez le mot de passe de l'administrateur.
   Le mot de passe par défaut est **admin**.
4. Effectuez l'une des tâches suivantes :

| Tâche | Environnement | Étapes |
|---|---|---|
| Vérifiez la configuration de l'interface réseau. | vSphere<br>ESXi | Saisissez `sudo /var/lib/cylance-gateway/scripts/configure-network --ovfenv --check`. Appuyez sur la touche **Entrée**. À l'invite, saisissez le mot de passe administrateur. |
| Modifiez la disposition du clavier dans le connecteur. | Tout | Par défaut, Ubuntu prend uniquement en charge les dispositions de clavier américaines.<br>**a.** Pour sélectionner une nouvelle disposition de clavier, saisissez `sudo dpkg-reconfigure keyboard-configuration`. Appuyez sur la touche **Entrée**.<br>**b.** À l'invite, saisissez le mot de passe administrateur.<br>**c.** Suivez les invites à l'écran. |

#### Accéder au CylanceGATEWAY Connector à l'aide d'OpenSSH

**Remarque :** Par défaut, OpenSSH est activé dans l'AMI CylanceGATEWAY Connector AWS. N'effectuez pas cette tâche si vous installez le connecteur dans votre environnement AWS. Reportez-vous à la section Configurer votre pare-feu pour CylanceGATEWAY Connector pour poursuivre la configuration CylanceGATEWAY Connector.

OpenSSH est préinstallé sur l'image du connecteur et vous permet d'accéder au CylanceGATEWAY Connector et d'effectuer des opérations système et des opérations de maintenance à l'aide du protocole SSH. Par défaut, le service OpenSSH est désactivé. Vous devez activer le service OpenSSH et générer les clés d'hôte chaque fois que vous accédez à une instance CylanceGATEWAY Connector à l'aide d'OpenSSH. Dans les environnements Microsoft Entra ID, le trafic TCP entrant doit être autorisé.

**Avant de commencer :** Vérifiez que le port 22 (SSH), le port 80 (HTTP) et le port 443 (HTTPS) sont ouverts et que le groupe de sécurité a accès à CylanceGATEWAY Connector à partir du réseau auquel l'inscription est connectée.

1. Effectuez l'une des opérations suivantes pour ouvrir la console dans votre environnement.

| Environnement | Description |
|---|---|
| vSphere | **a.** Connectez-vous à votre environnement.<br>**b.** Cliquez sur le nom d'hôte du CylanceGATEWAY Connector.<br>**c.** Cliquez sur **Lancer la console à distance** ou sur **Lancer la console Web**. |
| ESXi | **a.** Connectez-vous à votre environnement.<br>**b.** Cliquez sur le nom d'hôte du CylanceGATEWAY Connector.<br>**c.** Cliquez sur **Console**. |

| Environnement | Description |
| --- | --- |
| Microsoft Entra ID | **a.** Connectez-vous au portail de gestion Microsoft Entra ID à l'adresse https://portal.azure.com.<br>**b.** Cliquez sur **Machines virtuelles**.<br>**c.** Cliquez sur le connecteur que vous avez créé dans Installer le CylanceGATEWAY Connector dans un environnement Microsoft Entra ID, étape 5.<br>**d.** Dans le menu de gauche, dans la section **Support + dépannage**, cliquez sur **Console série**.<br>**e.** Dans la colonne de gauche, cliquez sur **Diagnostics de démarrage**.<br>**f.** Cliquez sur l'onglet **Paramètres**.<br>**g.** Sélectionnez **Activer avec un compte de stockage personnalisé**.<br>**h.** Dans la liste déroulante **Compte de stockage de diagnostic**, sélectionnez le compte de stockage que vous avez créé dans Installer le CylanceGATEWAY Connector dans un environnement Microsoft Entra ID, étape 3.<br>**i.** Cliquez sur **Enregistrer**.<br>**j.** Sur l'écran du connecteur, dans le menu de gauche, dans la section **Support + dépannage**, cliquez sur **Console série**. |
| Hyper-V | **a.** Ouvrez le gestionnaire Hyper-V.<br>**b.** Cliquez avec le bouton droit de la souris sur le connecteur auquel vous souhaitez accéder **> Connecter**. |

2. À l'invite UNIX, saisissez le nom d'utilisateur de l'administrateur et appuyez sur **Entrée**. La valeur par défaut est admin.
3. Saisissez le mot de passe de l'administrateur. Le mot de passe par défaut est admin.
4. Générez les clés d'hôte pour le service OpenSSH. Saisissez `sudo dpkg-reconfigure openssh-server`. Appuyez sur la touche **Entrée**.
5. À l'invite, saisissez le mot de passe administrateur.
6. Activez le service OpenSSH. Saisissez `sudo systemctl --system enable ssh`. Appuyez sur la touche **Entrée**.

   **Remarque :** Cette commande ne démarre pas le service.
7. Démarrez le service OpenSSH. Saisissez `sudo systemctl --system start ssh`. Appuyez sur la touche **Entrée**.
8. Vous pouvez effectuer l'une des actions suivantes (facultatif) :

| Tâche | Étapes |
| --- | --- |
| Désactivez le démarrage du service OpenSSH pendant le démarrage du système. | Saisissez `sudo systemctl --system disable ssh`. Cette commande n'arrête pas le service. |
| Arrêtez le service OpenSSH. | Saisissez `sudo systemctl --system stop ssh`. Appuyez sur la touche **Entrée**. |
| Vérifiez que le service OpenSSH est activé. | Saisissez `sudo systemctl --system is-enabled ssh`. |

| Tâche | Étapes |
| --- | --- |
| Vérifiez que le service OpenSSH fonctionne. | Saisissez `sudo systemctl --system is-active ssh`. |
| Obtenir l'état du service OpenSSH | Saisissez `sudo systemctl --system status ssh`. |

9. Quittez la console.
10. Si vous le souhaitez, dans un environnement Microsoft Entra ID, vous pouvez désactiver les paramètres de diagnostic de démarrage de la machine virtuelle du connecteur que vous avez configurée à l'étape 1.

#### Configurer votre pare-feu pour CylanceGATEWAY Connector

Le CylanceGATEWAY Connector s'exécute à l'intérieur de votre réseau privé, derrière votre pare-feu, et dispose d'une adresse IP privée. Il se connecte au service cloud CylanceGATEWAY avec HTTPS et UDP. Le CylanceGATEWAY Connector doit pouvoir se connecter à CylanceGATEWAY via votre pare-feu (via NAT).

Le CylanceGATEWAY Connector doit pouvoir utiliser DNS pour résoudre les FQDN CylanceGATEWAY publics en adresses IP Internet. Le CylanceGATEWAY Connector utiliser le système utilise vos serveurs DNS privés pour réaliser ceci.

L'agent CylanceGATEWAY communique avec la console de gestion via des Websockets sécurisés (WSS) et doit être en mesure d'établir cette connexion directement. Pour que l'agent CylanceGATEWAY puisse s'activer et s'authentifier régulièrement, vous devez autoriser l'accès aux domaines appropriés (par exemple, idp.blackberry.com et le domaine de votre région). Si votre environnement utilise un proxy d'authentification, vous devez autoriser le trafic sur le serveur proxy.

Pour plus d'informations sur les FQDN, les ports, les plages d'adresses IP et les autres exigences en matière de pare-feu, visitez le site support.blackberry.com/community pour lire l'article 79017. Pour en savoir plus sur la configuration réseau requise pour Cylance Endpoint Security, consultez la section Configuration réseau requise pour Cylance Endpoint Security.

#### Inscrivez le CylanceGATEWAY Connector auprès de BlackBerry Infrastructure

Une fois que vous avez installé le connecteur CylanceGATEWAY Connector et configuré son pare-feu, vous devez le connecter à BlackBerry Infrastructure.

1. Dans un navigateur Web, accédez à l'adresse IP de votre connecteur CylanceGATEWAY Connector.
2. Pour accepter le certificat auto-signé et accéder au service HTTPS, cliquez sur **Continuer vers le service HTTPS**.
3. Lorsque l'invite s'affiche, saisissez le nom d'utilisateur et le mot de passe par défaut de l'administrateur, puis cliquez sur **Connexion**.

   La valeur par défaut est admin. Le mot de passe par défaut est blackberry.
4. La première fois que vous vous connectez à l'interface Web CylanceGATEWAY Connector, vous devez modifier le mot de passe administrateur par défaut du CylanceGATEWAY Connector. Cela ne modifie pas le mot de passe pour le CylanceGATEWAY Connector dans le ESXi, vSphere, le portail Microsoft Entra ID, la console AWS ou la console de gestion Hyper-V.
5. Connectez-vous à nouveau à l'interface Web CylanceGATEWAY Connector à l'aide du nouveau mot de passe.
6. Sur l'écran **Contrat de licence de la solution BlackBerry**, lisez le contrat de licence et cliquez sur **J'accepte**.
7. Pour autoriser le CylanceGATEWAY Connector pour BlackBerry Infrastructure dans votre organisation, vous devez inscrire le connecteur.

a) Lisez et acceptez la déclaration de confidentialité. Cochez la case **J'accepte la politique de confidentialité de BlackBerry**.
b) Dans le champ **URL**, saisissez l'URL du connecteur pour accéder à la console de gestion.

   Pour obtenir l'URL, dans la console de gestion, cliquez sur **Paramètres > Réseau > Réseau privé**, puis sur l'onglet **Connecteurs Gateway** et cliquez sur **Ajouter des connecteurs**.
c) Dans le champ **URL du proxy**, saisissez l'URL du serveur proxy. Lorsque vous saisissez l'URL du proxy sur cet écran, le champ **URL du proxy** sur la page Paramètres est renseigné avec la même URL et vice versa.

8. Cliquez sur **Inscrire ce connecteur**. La console de gestion s'ouvre.
9. Connectez-vous à la console de gestion en tant qu'administrateur.
10. Dans le champ **Nom du connecteur**, saisissez un nom.
11. Dans la liste déroulante **Groupe de connecteurs**, sélectionnez le groupe de connecteurs auquel vous souhaitez l'attribuer.
12. Cliquez sur **Autoriser**.

Le connecteur, sa version et le groupe de connecteurs auquel il est affecté figurent dans la liste des connecteurs CylanceGATEWAY. La colonne **État** indique si le réseau privé, son DNS et les contrôles d'intégrité fonctionnent normalement. Pour plus d'informations sur les états qui peuvent s'afficher, reportez-vous à la section Gestion de CylanceGATEWAY Connectors

**À la fin :** Si le CylanceGATEWAY Connector est inscrit, mais que son tunnel n'est pas connecté à la BlackBerry Infrastructure, vous pouvez lancer un test de connectivité pour vérifier si le système BlackBerry Infrastructure a reçu les paquets UDP envoyés depuis votre réseau privé, et que votre réseau privé a reçu les paquets UDP envoyés depuis le système BlackBerry Infrastructure. Dans l'invite de connexion de votre environnement (par exemple, vSphere) Saisissez `/var/lib/cylance-gateway/bin/udp-connectivity-test`. Appuyez sur la touche **Entrée**. Vous pouvez exécuter cette commande dans le shell de votre choix (par exemple, csh et bash). Pour en savoir plus sur les résultats de connectivité, reportez-vous à la section Réponses du test de connectivité UDP.

#### Afficher les détails d'un CylanceGATEWAY Connector inscrit

Vous pouvez afficher les détails de CylanceGATEWAY Connector une fois qu'il est inscrit dans l'interface Web de CylanceGATEWAY Connector. Si votre réseau dispose de plusieurs instances de CylanceGATEWAY Connector, vous devez accéder à l'interface Web pour chaque instance. Vous pouvez afficher l'état de tous les connecteurs de votre environnement dans la console de gestion.

- Lorsque le connecteur est inscrit auprès de BlackBerry Infrastructure, vous pouvez afficher les informations suivantes. Vous pouvez cliquer sur **Gérer ce connecteur** pour ouvrir la console de gestion Cylance Endpoint Security et gérer les connecteurs CylanceGATEWAY Connector.
  - Identifiants CylanceGATEWAY Connector utilisés par BlackBerry Infrastructure pour identifier l'instance
  - État actuel et informations d'enregistrement de l'instance
  - Nombre de tunnels connectés à BlackBerry Infrastructure par le CylanceGATEWAY Connector
- Vous pouvez télécharger les fichiers journaux. Les fichiers journaux sont téléchargés dans votre dossier Téléchargements dans un fichier zip pouvant contenir plusieurs fichiers journaux CylanceGATEWAY Connector. Cliquez sur **Télécharger les journaux**. Extrayez les journaux pour les consulter ou envoyez le fichier zip au support BlackBerry pour résoudre les problèmes potentiels. Les fichiers journaux de chaque instance peuvent également être téléchargés à partir de la console de gestion à partir du volet d'informations sur le connecteur de la page de CylanceGATEWAY Connector.
- Vous pouvez configurer le connecteur CylanceGATEWAY.

### Configurer le CylanceGATEWAY Connector

Vous pouvez effectuer diverses tâches dans l'interface Web CylanceGATEWAY Connector. Si plusieurs instances du CylanceGATEWAY Connector sont installées et configurées sur votre réseau, les tâches doivent être effectuées sur chaque instance CylanceGATEWAY Connector de votre environnement, si nécessaire. Vous pouvez afficher l'état de tous les connecteurs de votre environnement sur la page Connecteurs Gateway de la console de gestion. Vous pouvez afficher l'état de chaque CylanceGATEWAY Connector dans votre navigateur Web. Pour plus d'informations, reportez-vous à : Afficher les détails d'un CylanceGATEWAY Connector inscrit

**Avant de commencer :** Vérifiez si une ou plusieurs instances CylanceGATEWAY Connector sont déployées.

1. Dans un navigateur Web, accédez à l'adresse IP de votre connecteur CylanceGATEWAY Connector.
2. Saisissez vos informations d'identification et cliquez sur **connexion**.
3. Effectuez l'une des tâches suivantes :

| Tâches | Étapes |
| --- | --- |
| Modifiez les paramètres. | Vous pouvez définir un ou plusieurs des paramètres suivants (facultatif).<br>**a.** Cliquez sur **Paramètres**.<br>**b.** Configurez un ou plusieurs des paramètres suivants :<br>• Générer un nouveau certificat TLS auto-signé : vous pouvez régénérer le certificat TLS à tout moment. Par défaut, le certificat est valable un an. L'interface Web affiche le jour et l'heure d'expiration du certificat, le numéro de série et l'hôte lié au certificat. Chaque fois que vous générez un nouveau certificat TLS, vous êtes invité à accepter le nouveau certificat.<br>• Configuration du proxy HTTP/S : si votre environnement est configuré avec un serveur proxy non authentifié utilisé pour les requêtes HTTP et HTTPS destinées à Internet, vous pouvez saisir l'URL du proxy. Lorsque l'URL du proxy est ajoutée, les requêtes HTTPS envoyées à BlackBerry Infrastructure par le CylanceGATEWAY Connector utilisent le proxy. Le trafic de tunnel n'utilisera pas le proxy.<br>• Configuration MTU (Maximum Transfer Unit) : par défaut, le CylanceGATEWAY Connector détecte automatiquement la MTU de votre réseau. Dans certains cas, vous devrez peut-être spécifier la valeur MTU que le CylanceGATEWAY Connector peut utiliser. BlackBerry recommande d'utiliser la détection automatique.<br>**Remarque :** Si vous spécifiez la MTU et souhaitez utiliser la détection automatique, vous devez redémarrer le CylanceGATEWAY Connector depuis votre environnement vSphere, Hyper-V, Microsoft Entra ID, AWS ou ESXi.<br>• Configuration NTP (Network Time Protocol) : par défaut, le système CylanceGATEWAY Connector utilise le serveur ntp.ubuntu.com d'Ubuntu pour la synchronisation de l'heure. Vous pouvez spécifier un serveur NTP personnalisé.<br>• Configuration APT (Advanced Package Tool) : par défaut, le CylanceGATEWAY Connector utilise les hôtes de référentiel d'Ubuntu, archive.ubuntu.com et security.ubuntu.com. Pour plus d'informations, rendez-vous sur support.blackberry.com/community et consultez l'article 79017. Vous pouvez spécifier un référentiel de packages personnalisé utilisé par le CylanceGATEWAY Connector. Notez que les mises à jour de sécurité sont appliquées automatiquement et que vous devez redémarrer le CylanceGATEWAY Connector dans la console de gestion pour que les mises à jour prennent effet.<br>**c.** Effectuez l'une des opérations suivantes :<br>• Cliquez sur **Mettre à jour les paramètres** pour enregistrer les modifications sur l'écran Paramètres.<br>• Cliquez sur **Restaurer les paramètres par défaut** pour restaurer tous les paramètres par défaut. Vous devez saisir vos informations d'identification pour que les modifications prennent effet. La connectivité réseau peut être interrompue (par exemple, si vous spécifiez une MTU, le CylanceGATEWAY Connector doit être redémarré).<br>• Cliquez sur **Réinitialisation des paramètres d'usine** pour effacer toutes les configurations CylanceGATEWAY Connector, y compris le certificat TLS auto-signé. Le CylanceGATEWAY Connector doit être redémarré et entraînera une interruption de la connectivité réseau. |

| Tâches | Étapes |
| --- | --- |
| Modifiez le mot de passe de l'administrateur. | Vous pouvez modifier le mot de passe de l'administrateur du CylanceGATEWAY Connector à tout moment. Cela ne modifie pas le mot de passe administrateur utilisé pour l'accès au CylanceGATEWAY Connector dans l'environnement vSphere, Hyper-V, Microsoft Entra ID, AWS ou ESXi. Chaque fois que vous modifiez le mot de passe, vous êtes invité à vous reconnecter à l'aide du nouveau mot de passe.<br>**a.** Cliquez sur **Modifier le mot de passe administrateur**.<br>**b.** Saisissez le mot de passe administrateur actuel.<br>**c.** Saisissez et confirmez le nouveau mot de passe.<br>**d.** Cliquez sur **Modifier le mot de passe**.<br>**e.** Lorsque vous y êtes invité, cliquez sur **Se connecter maintenant**. Vous serez également automatiquement redirigé vers l'invite de connexion après un bref délai.<br>**f.** Saisissez votre nom d'utilisateur administrateur et votre nouveau mot de passe, puis cliquez sur **Connexion**. |

#### Gestion de CylanceGATEWAY Connectors

Après avoir enregistré CylanceGATEWAY Connectors, vous pouvez spécifier une URL de contrôle d'intégrité et limiter les adresses IP de vos connecteurs. Si aucune URL de contrôle d'intégrité n'est spécifiée, les informations DNS et HTTP ne s'affichent pas dans l'état du contrôle d'intégrité d'un connecteur. Pour les CylanceGATEWAY Connectors, procédez de l'une des façons suivantes :

| Écran | Actions |
| --- | --- |
| Sur l'écran de la liste des connecteurs Gateway | • Afficher le nombre de connexions actives.<br>• Affichez le groupe de connecteurs auquel le CylanceGATEWAY Connector appartient.<br>• Affichez des métadonnées de contrôle d'intégrité supplémentaires pour chaque instance de connecteur.<br>• Afficher la version de chaque instance de connecteur.<br>• Afficher l'état de vos connecteurs.<br>• Recharger les informations relatives aux CylanceGATEWAY Connectors.<br>• Télécharger les fichiers journaux de chaque instance de connecteur.<br>• Désactiver un connecteur pour éviter que de nouvelles connexions ne passent par le connecteur. Les connexions réseau actives ne sont pas interrompues. |

| Écran | Actions |
| --- | --- |
| Sur la page d'informations relatives au connecteur | • Affichez le groupe de connecteurs auquel le CylanceGATEWAY Connector appartient.<br>• Modifier le champ d'URL privée d'un connecteur et ouvrir l'URL dans une autre page.<br>• Affectez le connecteur à un autre groupe de connecteurs.<br>• Désactiver un connecteur pour éviter que de nouvelles connexions ne passent par le connecteur. Les connexions réseau actives ne sont pas interrompues.<br>• Afficher la version du connecteur.<br>• Afficher l'état de la connexion du connecteur.<br>• Télécharger les fichiers journaux du connecteur.<br>• Afficher la clé publique.<br>• Afficher l'historique des connexions du connecteur. L'heure de l'historique des connexions est en UTC. |

La restriction des adresses IP sources fournit une sécurité supplémentaire pour garantir que seuls les CylanceGATEWAY Connectors avec les adresses IP que vous spécifiez peuvent se connecter à votre réseau privé. Si vous limitez les adresses IP sources, vos CylanceGATEWAY Connectors doivent disposer d'une adresse IP fixe, soit en définissant une adresse IP statique pour le CylanceGATEWAY Connector lors de son déploiement dans un environnement vSphere ou un environnement ESXi, soit en créant une réservation d'IP DHCP sur votre réseau.

En fonction du nombre d'utilisateurs actifs de CylanceGATEWAY dans votre environnement, un composant du BlackBerry Infrastructure responsable de la gestion des tunnels entrants à partir du connecteur peut faire évoluer les ressources allouées à votre entreprise. Chaque CylanceGATEWAY Connector établit un tunnel vers ce composant et fait l'objet d'un contrôle d'intégrité. Les colonnes État du contrôle d'intégrité et État fournissent ensuite une indication de l'état de ces tunnels, du connecteur au composant responsable de leur gestion. Par exemple, si la colonne Contrôle d'intégrité indique l'état $X$/2, cela signifie que deux des composants sont affectés à votre organisation à ce moment-là. Si la colonne affiche 2/2, cela signifie que le connecteur a réussi à établir deux tunnels vers le composant. Si vous voyez 0/2 ou 1/2, cela signifie que le connecteur n'a pas établi de tunnel ou a établi 1 des 2 tunnels requis. Si l'état est ⚠, certains de vos utilisateurs peuvent accéder aux ressources de votre réseau privé, mais pas tous.

L'URL de contrôle d'intégrité peut être une URL quelconque au sein de vos réseaux privés auxquels vous souhaitez que les utilisateurs CylanceGATEWAY puissent se connecter. CylanceGATEWAY envoie régulièrement une demande GET HTTP ou HTTPS, comprenant une recherche DNS, via chaque tunnel CylanceGATEWAY Connector vers cette URL. L'état du contrôle d'intégrité se développe pour afficher l'état de la connexion du tunnel, DNS et HTTP de chaque connecteur. Un état 2/2 indique que tout fonctionne correctement. L'état 0/0 indique que le contrôle d'intégrité d'une nouvelle connexion est toujours en attente.

La colonne État affiche l'état d'inscription du CylanceGATEWAY Connector avec BlackBerry Infrastructure. ✔ indique que le CylanceGATEWAY Connector a terminé le processus d'inscription et qu'il a établi une connexion avec BlackBerry Infrastructure. La colonne État affiche l'état de la connexion et peut inclure un message de sécurité (par exemple, si le connecteur nécessite un redémarrage pour appliquer une mise à jour).

| Colonne | Description |
| --- | --- |
| État du contrôle d'intégrité | Il s'agit de l'état global du CylanceGATEWAY Connector, qui inclut les informations suivantes :<br>• **Tunnel** : état de connexion du CylanceGATEWAY Connector à l'BlackBerry Infrastructure. Si l'état indique un problème de connexion, contactez votre représentant de l'assistance BlackBerry.<br>• **DNS** : état de la requête DNS effectuée depuis le CylanceGATEWAY Connector vers votre serveur DNS spécifié. Si l'état indique un problème, vérifiez que vous avez correctement spécifié votre serveur DNS privé.<br>• **HTTP** : état de la requête HTTP effectuée auprès du CylanceGATEWAY Connector pour l'URL de contrôle d'intégrité. Si l'état indique un problème, vérifiez que l'URL du contrôle d'intégrité est accessible par CylanceGATEWAY Connector et que vous avez spécifié une zone de recherche directe DNS. |
| État | Il s'agit de l'état global de la connexion du CylanceGATEWAY Connector à l'BlackBerry Infrastructure, notamment de l'état du contrôle d'intégrité.<br>• : le connecteur n'a pas terminé le processus d'inscription. Cet état s'affiche uniquement lorsque le connecteur est inscrit pour la première fois.<br>• : le connecteur a terminé le processus d'inscription et établit une connexion avec BlackBerry Infrastructure.<br>• : le connecteur a terminé le processus d'inscription, mais toutes les connexions à BlackBerry Infrastructure n'ont pas été établies. Si cet état s'affiche, lisez le message de sécurité associé et vérifiez qu'une URL de contrôle d'intégrité a été spécifiée dans le groupe de connecteurs.<br>• : le processus d'inscription du connecteur n'est pas terminé ou une erreur s'est produite lors de l'établissement de toutes les connexions à BlackBerry Infrastructure. Les messages d'erreur suivants peuvent s'afficher :<br>  • Échec de l'enregistrement en raison d'une erreur de stockage : vérifiez que vous disposez d'un espace disque suffisant pour enregistrer le CylanceGATEWAY Connector.<br>  • Échec : affichez l'état de contrôle d'intégrité complet du connecteur, y compris les informations relatives au tunnel ainsi qu'aux requêtes DNS et HTTP. Par exemple, si la requête DNS affiche « Échec », vérifiez que vos paramètres DNS sont corrects. |

#### Gestion des connecteurs CylanceGATEWAY

Effectuez cette tâche pour chaque groupe de connecteurs.

1. Sur la barre de menus de la console de gestion, cliquez sur **Paramètres > Réseau**.
2. Cliquez sur l'onglet **Réseau privé**.
3. Cliquez sur **Groupes de connecteurs**. Cliquez sur un groupe de connecteurs.
4. Cliquez sur **Contrôle d'intégrité**.
5. Spécifiez une URL dans votre réseau privé à laquelle CylanceGATEWAY Connector peut accéder pour vérifier que CylanceGATEWAY peut s'y connecter.

   L'URL du contrôle d'intégrité doit contenir un FQDN que votre serveur DNS privé peut résoudre. Le FQDN doit être résolu en une adresse IP comprise dans l'espace IP défini pour votre réseau privé.

6. Pour spécifier les adresses IP autorisées pour vos CylanceGATEWAY Connectors, cliquez sur **Restriction d'IP source**.
7. Cliquez sur **Ajouter**.
8. Cliquez sur **Enregistrer**.
9. Pour afficher des informations supplémentaires sur un CylanceGATEWAY Connector et pour télécharger les fichiers journaux du connecteur ou saisir un FQDN ou une adresse IP personnalisés dans l'URL privée, cliquez sur le nom du CylanceGATEWAY Connector.

   **Remarque :** Si vous saisissez un FQDN ou une adresse IP personnalisé(e), le FQDN ou l'adresse IP n'est pas validé(e).
10. Pour recharger les informations concernant le CylanceGATEWAY Connectors, cliquez sur ↻.

#### Mettre à jour un CylanceGATEWAY Connector

Vous pouvez vérifier si une mise à jour pour le CylanceGATEWAY Connector ou une mise à jour pour le système d'exploitation de la machine virtuelle est disponible.

**Avant de commencer :** Vérifiez la version du CylanceGATEWAY Connector installée dans la console de gestion Cylance Endpoint Security, sous Paramètres > Réseau > Réseau privé > Connecteurs Gateway.

1. Vérifiez sur *my*Account ou les Notes de version de Cylance Endpoint Security si une nouvelle version du logiciel CylanceGATEWAY Connector est disponible et effectuez l'une des opérations suivantes :
   - Si un nouveau logiciel CylanceGATEWAY Connector est disponible, effectuez l'étape 2 correspondant à votre environnement.
   - Si aucune nouvelle mise à jour logicielle du CylanceGATEWAY Connector n'est disponible, recherchez une mise à jour du système d'exploitation Linux.
2. Effectuez l'une des tâches suivantes :

| Environnement | Étapes |
|---|---|
| Mettez à jour CylanceGATEWAY Connector version 2.9 ou version ultérieure. | Utilisez le fichier DEB pour mettre à jour l'instance de connecteur et conserver vos configurations.<br>**a.** Dans *my*Account, téléchargez la version DEB du connecteur.<br>**b.** Copiez le package DEB sur le connecteur à mettre à niveau. Si SSH est activé, vous pouvez utiliser SCP pour copier le package DEB à partir d'un hôte disposant d'un accès SSH au connecteur. Pour obtenir des instructions, reportez-vous à Accéder au CylanceGATEWAY Connector à l'aide d'OpenSSH. Sinon, vous pouvez utiliser SCP sur le connecteur pour copier le package DEB à partir d'un hôte SSH auquel le connecteur peut accéder.<br>**c.** Dans la console Unix, saisissez `sudo apt install <path>/cylance-gateway-connector-<version>.deb`.<br>Par exemple, `sudo apt install /home/admin/cylance-gateway-connector-2.10.0.938.deb`<br>**d.** Appuyez sur la touche **Entrée**. |

| Environnement | Étapes |
| --- | --- |
| Mettez à jour CylanceGATEWAY Connector version 2.8 ou antérieure ou effectuez une réinstallation complète. | Créez une nouvelle instance du connecteur pour votre environnement. Pour obtenir des instructions, consultez la section Installation du connecteur CylanceGATEWAY. |

3. Pour tout CylanceGATEWAY Connector affichant **Redémarrage requis pour appliquer les mises à jour du système d'exploitation et les correctifs de sécurité** dans la colonne **État**, redémarrez la machine virtuelle pour terminer l'installation de la mise à jour du système d'exploitation.

**À la fin :** Si le CylanceGATEWAY Connector est inscrit, mais que son tunnel n'est pas connecté à la BlackBerry Infrastructure, vous pouvez lancer un test de connectivité pour vérifier si le système BlackBerry Infrastructure a reçu les paquets UDP envoyés depuis votre réseau privé, et que votre réseau privé a reçu les paquets UDP envoyés depuis le système BlackBerry Infrastructure. Dans l'invite de connexion de votre environnement (par exemple, vSphere), saisissez `/var/lib/cylance-gateway/bin/udp-connectivity-test`. Appuyez sur la touche **Entrée**. Vous pouvez exécuter cette commande dans le shell de votre choix (par exemple, csh et bash). Pour en savoir plus sur les résultats de connectivité, reportez-vous à la section Réponses du test de connectivité UDP.

#### Réponses du test de connectivité UDP

Les exemples suivants illustrent les sorties qui peuvent s'afficher lorsque vous vérifiez le chemin UDP entre CylanceGATEWAY Connector et BlackBerry Infrastructure.

Dans les exemples suivants :

- Endpoint correspond à l'adresse IP et au port du test udp-connectivity-test effectué.
- Client Address:Port correspond à l'adresse IP externe et le port du CylanceGATEWAY Connector , tels qu'ils sont vus par la BlackBerry Infrastructure.
- Server correspond à BlackBerry Infrastructure.

#### Exemple : le trafic UDP a bien été envoyé et reçu

Dans cet exemple, le trafic UDP est correctement envoyé et reçu entre le connecteur de votre réseau privé et la BlackBerry Infrastructure.

```
Initiating discovery request
Starting connectivity test using endpoint=<IP address>:<port>
Sent hello message with id='62f6bf9e-741c-4f22-9907-2725789aa318' to <IP
 address>:<port>
Waiting for server hello
Received server hello with id='62f6bf9e-741c-4f22-9907-2725789aa318' from <IP
 address>:<port>
Sent ack message with id='62f6bf9e-741c-4f22-9907-2725789aa318' to <IP
 address>:<port>
Report:
  Client Address:Port = <IP address>:<port>
  Packet Size       = 1500
  Fragmented        = false
  RTT               = 3ms
```

#### Exemple : le trafic UDP sortant est bloqué

Dans cet exemple, le client de test de connectivité UDP a pu envoyer hello, mais la BlackBerry Infrastructure n'a pas reçu la réponse avant l'expiration du délai.

```
Initiating discovery request
Starting connectivity test using endpoint=<IP address>:<port>
Sent hello message with id='2dca5fcf-3f9a-46c3-a158-911a851f94a7' to <IP
 address>:<port>
Waiting for server hello
Error: Timeout on receiving server hello
Getting test report from server
Error: The server did not receive our hello message.  Is outbound UDP blocked?
Starting connectivity test using endpoint=<IP address>:<port>
Sent hello message with id='40fe1e15-b2c0-4607-9880-7be08ec505ac' to <IP
 address>:<port>
Waiting for server hello
Error: Timeout on receiving server hello
Getting test report from server
Error: The server did not receive our hello message.  Is outbound UDP blocked?
Error: No endpoints to test
```

#### Exemple : le trafic UDP entrant est bloqué

Dans cet exemple, le client de test de connectivité UDP a envoyé le test de connectivité UDP hello et la BlackBerry Infrastructure l'a reçu et y a répondu, mais le client de test n'a pas reçu la réponse avant l'expiration du délai.

```
Initiating discovery request
Starting connectivity test using endpoint=<IP address>:<port>
Sent hello message with id='973e0d45-71f0-427b-be08-9e5f16d03349' to <IP
 address>:<port>
Waiting for server hello
Error: Timeout on receiving server hello
Getting test report from server
Error: The server sent a response that was not received.  Is inbound UDP blocked?
Starting connectivity test using endpoint=99.83.155.194:58255
Sent hello message with id='2fc6d3f8-43c2-4707-bc77-e85168c2596e' to <IP
 address>:<port>
Waiting for server hello
Error: Timeout on receiving server hello
Getting test report from server
Error: The server sent a response that was not received.  Is inbound UDP blocked?
Error: No endpoints to test
```

### Spécifier votre réseau privé

**Avant de commencer :**

- Assurez-vous d'avoir une liste des adresses IP ou les plages d'adresses IP pour toutes les destinations que vous souhaitez définir dans le cadre de votre réseau privé. Vous pouvez obtenir ces informations auprès de votre administrateur réseau.
- Vous ne pouvez pas configurer l'accès au réseau privé si vous n'installez pas de CylanceGATEWAY Connector. Assurez-vous d'avoir installé un ou plusieurs CylanceGATEWAY Connectors dans une partie de chaque réseau disposant d'un accès complet aux adresses que vous spécifiez ici. Pour obtenir des instructions sur l'installation d'un CylanceGATEWAY Connector, consultez Installation du connecteur CylanceGATEWAY.

- Vous pouvez créer un maximum de huit groupes de connecteurs. Vous pouvez créer un maximum de huit CylanceGATEWAY Connector vers chaque groupe de connecteurs.

1. Sur la barre de menus, cliquez sur **Paramètres > Réseau**.
2. Cliquez sur l'onglet **Réseau privé**.
3. Cliquez sur **Groupes de connecteurs**.
4. Cliquez sur **Ajouter un groupe de connecteurs**.
5. Saisissez un nom et une description. Le nom du connecteur peut comporter entre 3 et 250 caractères. La description peut comporter entre 3 et 500 caractères.
6. Dans l'onglet **Routage réseau**, cliquez sur **Ajouter une adresse**.
7. Saisissez une ou plusieurs adresses IP, plages IP ou CIDR et cliquez sur **Ajouter**.

   Si votre environnement exige que l'ensemble du trafic réseau soit redirigé vers votre infrastructure sur site, saisissez `0.0.0.0/0`. BlackBerry vous recommande de rediriger uniquement le trafic destiné aux ressources de votre réseau privé, puis de configurer votre environnement pour qu'il utilise les services cloud CylanceGATEWAY pour le trafic vers les destinations Internet.

   **Remarque :** Lorsque vous spécifiez 0.0.0.0/0 pour votre routage réseau, l'ensemble du trafic non DNS (par exemple, le trafic HTTP) est acheminé via le CylanceGATEWAY Connector. Pour acheminer le trafic vers des ressources qui ne font pas partie de votre réseau privé, la requête DNS doit être envoyée à des serveurs DNS publics, et non à votre serveur DNS privé, avant que la connexion soit établie et que le trafic soit acheminé via le CylanceGATEWAY Connector.
8. Pour modifier une adresse, cliquez sur en regard de l'adresse.
9. Pour supprimer une adresse, cliquez sur ✕ en regard de l'adresse.
10. Pour modifier l'ordre de la liste, faites glisser ⠿ du groupe de connecteurs vers l'emplacement approprié de la liste.
11. Pour supprimer un groupe de connecteurs, supprimez ou réaffectez tous les CylanceGATEWAY Connectors attribués du groupe de connecteurs. Cliquez sur .

## Spécifier votre DNS privé

Vous pouvez fournir les paramètres de votre DNS privé pour aider CylanceGATEWAY à acheminer le trafic au sein de votre réseau privé. Vous pouvez spécifier les adresses IP de vos serveurs DNS, les noms de domaine délégués à vos serveurs DNS pour les recherches directes ainsi que les CIDR délégués à vos serveurs DNS pour les recherches inversées. Les adresses IP du serveur DNS sont partagées par tous les groupes de connecteurs et doivent être incluses dans un groupe de connecteurs. Vous pouvez obtenir ces informations auprès de votre administrateur réseau.

1. Sur la barre de menus, cliquez sur **Paramètres > Réseau**.
2. Cliquez sur l'onglet **Réseau privé**.
3. Cliquez sur **DNS**.
4. Pour spécifier un serveur DNS, procédez comme suit :
   a) Cliquez sur **Serveurs DNS**.
   b) Cliquez sur **Ajouter un serveur DNS**.
   c) Saisissez l'adresse IP de votre serveur DNS et cliquez sur **Ajouter**.
5. Pour spécifier un domaine pour les recherches directes, procédez comme suit : Vous pouvez spécifier un maximum de 100 zones de recherche directe.
   a) Cliquez sur **Zone de recherche directe**.
   b) Cliquez sur **Ajouter une zone directe**.
   c) Entrez un nom de domaine et cliquez sur **Ajouter**.

Si vous ne spécifiez pas de zone de recherche directe, le contrôle d'intégrité du CylanceGATEWAY Connector échoue. Si vous activez la tunnellisation fractionnée, mais que vous ne spécifiez pas de zone de recherche directe, toutes les requêtes DNS transitent par le tunnel.

6. Pour spécifier un CIDR pour les recherches inversées, effectuez les actions suivantes :
   a) Cliquez sur **Zone de recherche inversée**.
   b) Cliquez sur **Ajouter une zone inversée**.
   c) Entrez un CIDR et cliquez sur **Ajouter**.
7. Pour modifier une adresse ou un nom de domaine, cliquez sur .
8. Pour supprimer une adresse ou un nom de domaine, cliquez sur .

## Spécifier vos suffixes DNS

Vous pouvez spécifier jusqu'à 32 suffixes que votre DNS privé ajoute à la recherche de noms non qualifiés. Vous pouvez obtenir ces informations auprès de votre administrateur réseau. Si vous spécifiez plusieurs suffixes, vous pouvez les classer.

1. Sur la barre de menus, cliquez sur **Paramètres > Réseau**.
2. Cliquez sur l'onglet **Client DNS**.
3. Activez **Domaine de recherche DNS (ou suffixe)**.
4. Cliquez sur **Ajouter un suffixe DNS**.
5. Saisissez le nom du suffixe DNS et cliquez sur **Ajouter**.
6. Répétez les étapes 4 et 5 pour chaque suffixe à ajouter.
7. Pour modifier un suffixe, cliquez sur .
8. Pour supprimer un suffixe, cliquez sur .
9. Pour modifier l'ordre de la liste, faites glisser pour le suffixe vers l'emplacement approprié de la liste.
10. Cliquez sur **Enregistrer**.

## Spécifiez les plages IP de l'agent privé CylanceGATEWAY

CylanceGATEWAY alloue des adresses IP privées de tunnel aux agents CylanceGATEWAY à partir d'une plage d'adresses IP privées configurée à l'échelle du système et identique pour chaque locataire. Vous pouvez spécifier une plage d'adresses IP privées de tunnel de point de terminaison qui ne chevauche pas la plage de réseau privé du locataire avec les agents CylanceGATEWAY. La fourniture d'une plage d'adresses IP privées peut empêcher des conflits potentiels, par exemple lorsqu'un agent tente d'accéder à un service de réseau privé ayant la même adresse IP attribuée à l'agent. La plage d'adresses IP de l'agent doit être au format CIDR IPv4 et unique au sein de votre réseau privé pour éviter les problèmes de routage vers d'autres points finaux de votre réseau. Par défaut, la plage est 10.10.0.0/16. Les suffixes doivent être inférieurs à 17.

**Avertissement :** Si vous modifiez la plage IP de l'agent, les agents et connecteurs CylanceGATEWAY Connector associés peuvent se déconnecter et se reconnecter. Si vous accédez à l'écran connecteurs de passerelle (Paramètres > Réseau > Réseau privé) pendant la déconnexion et la reconnexion, l'un des messages suivants peut s'afficher. Cliquez sur .

- L'enregistrement n'a pas pu être terminé : 500
- Échec. Le redémarrage est requis pour appliquer les mises à jour du système d'exploitation et les correctifs de sécurité.

1. Sur la barre de menus, cliquez sur **Paramètres > Réseau**.
2. Cliquez sur l'onglet **Réseau privé**.
3. Cliquez sur **Plage IP des agents**.
4. Saisissez l'adresse CIDR.

5. Cliquez sur **Enregistrer**.

### Apporter vos propres adresses IP (BYOIP)

Vous pouvez ajouter des adresses IP dédiées dans une plage CIDR/24 IPv4 à CylanceGATEWAY qui sont utilisées pour gérer le trafic de sortie réseau.

Vous pouvez utiliser les adresses IP dédiées pour effectuer les opérations suivantes :

- Utiliser les adresses IP de votre entreprise pour l'épinglage des adresses IP sources.
- Éviter les problèmes où certains sites Web bloquent les plages d'adresses IP AWS.
- Refléter les informations GeoIP relatives aux adresses.
- Autoriser un seul CIDR au lieu de plusieurs adresses IP non continues.

Pour ajouter des adresses IP dédiées à CylanceGATEWAY, vous soumettez une demande à BlackBerry Technical Support Services. Pour obtenir des instructions, rendez-vous sur le site https://support.blackberry.com/community et lisez l'article 100189.

# Traduction d'adresses réseau avec CylanceGATEWAY

Par défaut, CylanceGATEWAY applique la traduction d'adresses réseau (NAT) au flux de trafic vers votre réseau privé. NAT s'applique également à vos points de terminaison (par exemple, les terminaux) lorsque les utilisateurs accèdent à Internet et aux applications SaaS. Une fois la traduction NAT appliquée, l'adresse IP réelle est masquée et toutes les connexions entrantes vers un point de terminaison spécifique sont bloquées. NAT n'est pas disponible pour les flux qui n'utilisent pas le tunnel CylanceGATEWAY (par exemple, mode sans échec).

**Remarque :** Les connexions entrantes aux points de terminaison sont empêchées par CylanceGATEWAY (par exemple, vous ne pouvez pas établir de connexion aux points de terminaison à l'aide d'outils informatiques distants, tels que la connexion Bureau à distance).

NAT est appliquée au trafic qui traverse CylanceGATEWAY Connector vers votre réseau privé. Le connecteur fournit des informations supplémentaires sur les flux UDP et TCP qui s'affichent sur l'écran Événements réseau (CylanceGATEWAY > Événements). Vous pouvez identifier l'adresse IP source privée et le port source privé d'un événement qui a été bloqué ou identifié comme potentiellement malveillant. Pour en savoir plus, consultez les sections suivantes :

- Afficher la page Détails de l'évènement
- Flux de données : accès à un serveur d'applications ou de contenu sur votre réseau privé

NAT est appliqué par CylanceGATEWAY au trafic qui traverse le tunnel pour accéder aux destinations Internet et aux applications SaaS basées sur le cloud. Vous pouvez filtrer les événements en fonction de l'adresse IP du tunnel de passerelle utilisée par les utilisateurs pour accéder aux destinations externes. Pour en savoir plus, consultez les sections suivantes :

- Afficher la page Détails de l'évènement
- Flux de données : accès à une application cloud ou destinations Internet

# Définir des services réseau

Un service réseau est un groupe d'adresses (FQDN ou adresses IP) que vous pouvez utiliser pour simplifier la mise en place de règles de liste de contrôle d'accès (ACL). Lorsque vous créez des règles ACL, vous pouvez spécifier un service réseau au lieu de spécifier chaque adresse individuelle. BlackBerry gère et met régulièrement à jour les services réseau pour de nombreuses applications SaaS courantes afin de simplifier le processus pour vous. Vous pouvez définir des services réseau supplémentaires pour les applications publiques et privées. Vous

pouvez imbriquer des services réseau existants. Lorsque vous imbriquez des services réseau, les destinations de chaque service réseau ajouté sont référencées et vous avez accès à toutes les destinations contenues. Si une modification est apportée à l'un des services réseau combinés, elle est automatiquement répercutée immédiatement. Vous pouvez effectuer une recherche des services réseau que vous avez ajoutés. Pour plus d'informations sur les recherches, consultez Recherche de règles ACL et de services réseau.

1. Sur la barre de menus de la console de gestion, cliquez sur **Paramètres > Réseau**.
2. Cliquez sur l'onglet **Services réseau**.
3. Cliquez sur **Ajouter**.
4. Saisissez le nom et la description du service réseau.
5. Vous pouvez également cliquer sur **Services réseau** et sélectionner au moins service réseau.
6. Vous pouvez également cliquer sur **Adresse**. Saisissez une adresse IP, un FQDN ou un domaine générique pour la destination. Cliquez sur + pour ajouter d'autres adresses. Les formats d'adresse suivants sont pris en charge :
   - Plage d'adresses IP : de 172.16.10.0 à 172.16.10.255
   - Adresse IP unique : 172.16.10.2
   - Plage d'adresses IP : de 172.16.10.0 à 172.16.10.255
   - CIDR : 172.16.10.0/24
   - FQDN : domaine.exemple.com
   - Domaine avec caractère générique : *.exemple.com
7. Cliquez sur **Protocole**, sélectionnez un protocole à utiliser pour la tentative de connexion, et spécifiez un port unique ou une plage de ports à utiliser. Cliquez sur + pour ajouter d'autres protocoles et ports.
8. Répétez les étapes 6 et 7 pour ajouter des adresses et des ports supplémentaires.
9. Cliquez sur **Ajouter**.
10. Pour modifier un service réseau, cliquez sur le champ à modifier et apportez les modifications nécessaires. Vous ne pouvez pas modifier les services définis par BlackBerry.
11. Pour supprimer un service réseau, cliquez sur ✕ en regard du service, de l'adresse ou du port. Pour supprimer une adresse et une ligne de port, cliquez sur ✕ en regard de l'adresse de destination et de la ligne de port appropriées. Vous ne pouvez pas modifier les services définis par BlackBerry.

**À la fin :** Vous pouvez effectuer une recherche dans la liste des services réseau pour afficher les informations. Cliquez sur 🔍 et sélectionnez une ou plusieurs portées prédéfinies, une condition et spécifiez les critères. Cliquez sur le service réseau dont vous souhaitez afficher les paramètres. Cliquez sur ✕ pour réinitialiser la recherche.

# Contrôle de l'accès réseau

Définissez les ressources réseau auxquelles les terminaux inscrits dans CylanceGATEWAY peuvent se connecter à l'aide de la liste de contrôle d'accès (ACL). La liste ACL définit les destinations autorisées et bloquées sur les réseaux privés et publics. La liste ACL s'applique uniquement aux utilisateurs auxquels une stratégie de service Gateway est attribuée.

La liste ACL s'applique à tous les utilisateurs CylanceGATEWAY du locataire. Chaque tentative d'accès au réseau par un terminal est évaluée par rapport aux règles, dans l'ordre, pour chaque phase de connexion (recherche DNS, établissement de connexion et liaison TLS) jusqu'à ce qu'une règle correspondant à la tentative soit trouvée. La règle doit correspondre à toutes les propriétés spécifiées, y compris la destination ou catégories de destination, les utilisateurs ou groupes spécifiés et le niveau de risque déterminé pour la destination. La première règle de correspondance détermine si la tentative d'accès est bloquée ou autorisée à passer à la phase suivante. Une tentative d'accès autorisée à travers toutes ses phases peut être entièrement établie. Si une tentative d'accès

réseau ne correspond à aucune règle de la liste ACL, l'accès est bloqué. La liste de contrôle d'accès prend en charge 1 000 règles maximum.

## Appliquer des règles ACL

Les règles ACL s'appliquent à tous les utilisateurs CylanceGATEWAY du locataire. Les règles ACL évaluent chaque tentative d'accès au réseau dans l'ordre dans lequel elles sont affichées dans la console de gestion, de haut en bas. La règle par défaut sera toujours évaluée en dernier et si aucune des règles précédentes ne correspond, l'accès à toutes les ressources sera bloqué. La règle par défaut ne peut pas être désactivée ou modifiée

Lorsque vous créez les règles ACL, BlackBerry vous recommande de créer vos règles ACL et de vous assurer qu'elles s'affichent dans l'ordre suivant :

1. Bloquez l'accès au contenu Internet qui contient des catégories spécifiées CylanceGATEWAY
2. Bloquez l'accès aux services non catégorisés en fonction des besoins de votre entreprise
3. Autorisez l'accès aux services à l'échelle de l'entreprise dans le réseau privé
4. Autorisez l'accès à toutes les destinations Internet publiques
5. Par défaut

Le tableau suivant fournit des exemples de règles et leurs paramètres nécessaires :

| Règle | Description |
|---|---|
| Autoriser les utilisateurs à accéder aux destinations Internet publiques | Cette règle permet aux utilisateurs d'accéder à toute destination que votre organisation considère comme l'Internet public. Les utilisateurs ne pourront pas accéder aux adresses RFC1918 spécifiées.<br>Pour créer cette règle, vous pouvez spécifier les paramètres suivants :<br>• Dans la section **Actions**,<br>  • La liste déroulante **Actions** affiche **Autoriser**.<br>  • La case **Vérifier les tentatives d'accès par rapport à la protection du réseau** est cochée. Ce paramètre permet à la règle de passer les règles ACL, mais permet également une inspection plus approfondie par Gateway.<br>• Dans la section **Destination**,<br>  • La liste déroulante **Cible** affiche **Ne correspond pas**.<br>  • Dans le champ **Adresses et ports**, **Adresse**, saisissez les plages réseau RFC1918. |

| Règle | Description |
| --- | --- |
| Autoriser les utilisateurs à accéder au réseau privé | Cette règle permet à l'utilisateur d'accéder aux services réseau au sein de votre réseau privé.<br>Pour que les utilisateurs puissent accéder au réseau privé, les conditions préalables suivantes doivent être remplies :<br>• Assurez-vous que CylanceGATEWAY Connector est installé sur le réseau pour permettre au trafic d'atteindre votre réseau privé. Pour obtenir des instructions sur la manière d'installer CylanceGATEWAY Connector dans votre environnement, consultez Installation du connecteur CylanceGATEWAY.<br>• Assurez-vous que vous avez défini un service réseau contenant les ressources de réseau privé auxquelles vous souhaitez que les utilisateurs accèdent. Pour plus d'informations sur la manière de définir les services réseau, consultez Définir des services réseau.<br>Vous pouvez spécifier les paramètres suivants :<br>• Dans la section **Actions** :<br>  • La liste déroulante **Actions** affiche **Autoriser**.<br>  • Si vous le souhaitez, décochez la case **Vérifier les tentatives d'accès par rapport à la protection du réseau**. Aucune autre inspection ne sera effectuée par Gateway.<br>• Dans la section **Destination** :<br>  • La liste déroulante **Cible** affiche **Avec correspondance**.<br>  • Dans le champ **Services réseau**, sélectionnez le service réseau auquel les utilisateurs doivent accéder. |

## Paramètres de l'ACL

La liste ACL est une liste triée de règles qui détermine comment traiter les tentatives d'accès d'un utilisateur CylanceGATEWAY à une destination sur Internet ou sur votre réseau privé. Chaque règle inclut plusieurs paramètres qui peuvent spécifier des destinations, des utilisateurs et d'autres facteurs auxquels une règle peut correspondre, ainsi que les mesures à prendre en cas de correspondance. Si une tentative d'accès réseau ne correspond à aucune règle ACL, l'accès est bloqué.

Lorsque vous ajoutez ou modifiez des règles ACL, les mises à jour sont ajoutées à une liste de règles provisoires jusqu'à ce que vous les validiez. Chaque administrateur dispose de sa propre liste de règles provisoires. Lorsqu'un administrateur valide une mise à jour de règles, tous les autres administrateurs disposant d'une liste de règles provisoires seront avertis de la suppression ou de la mise à jour de leur liste de règles provisoires avant de continuer.

Chaque règle peut inclure les paramètres suivants :

| Élément | Description |
| --- | --- |
| **Informations générales** | |
| Nom | Il s'agit du nom de la règle. |
| Description | Il s'agit d'une brève description de l'objectif de la règle. |

| Élément | Description |
| --- | --- |
| Activé | Ce paramètre spécifie si la règle est comprise dans l'ACL. Vous pouvez désactiver cette option pour désactiver la règle sans la supprimer. |
| **Action** | |
| Action | Ce paramètre indique si l'accès doit être autorisé ou bloqué lorsque la tentative correspond à la règle. Si la tentative d'accès est autorisée à continuer, elle peut être réévaluée lors des phases suivantes de la tentative. |
| Vérifier les adresses par rapport à la protection réseau | Si l'action de règle autorise l'accès, ce paramètre spécifie si CylanceGATEWAY maintient le blocage de la connexion en cas de détection d'une potentielle menace sur le réseau. Laissez cette option sélectionnée sauf si des utilisateurs spécifiques doivent se connecter à des destinations potentiellement malveillantes. |
| Afficher un message de notification bloquée sur les terminaux | Si l'action de règle bloque l'accès, ce paramètre indique un message de notification qui s'affiche sur le terminal en cas de blocage d'une tentative d'accès. |
| Confidentialité du trafic | Ce paramètre spécifie si les tentatives d'accès au réseau sont affichées dans l'écran Évènements réseau (CylanceGATEWAY > Évènements). Vous pouvez activer la fonction Confidentialité du trafic pour des raisons de responsabilité ou de confidentialité. Lorsque ce paramètre est activé, les tentatives d'accès au réseau ne s'affichent pas dans l'écran Événements réseau. Si votre environnement envoie des évènements à une solution SIEM ou à un serveur syslog et que la tentative de connexion correspond à une règle de confidentialité du trafic, les évènements ne sont pas envoyés à la solution SIEM ou au serveur syslog. |
| Journalisation de contenu | Ce paramètre spécifie si la page Évènements réseau > Détails des évènements doit inclure des données de connexion HTTP non chiffrées en texte brut d'origine. Les flux HTTP ne sont pas déchiffrés. Lorsque ce paramètre est activé, un résumé des détails de la demande et de la réponse d'un évènement est inclus dans la page Détails des évènements. Vous pouvez afficher toutes les transactions HTTP d'un évènement. La page Détails des évènements inclut les trois premiers évènements HTTP du nombre total d'évènements. Vous pouvez afficher tous les évènements et les détails qui leur sont associés. Si vous créez une règle qui inclut à la fois la confidentialité du trafic et la journalisation du contenu, la confidentialité du trafic est prioritaire. |
| Ignorer le port | Ce paramètre indique si le port de destination de la tentative de contrôle d'accès doit être évalué ou ignoré dans le cadre de cette règle. |
| **Destinations** | |

| Élément | Description |
| --- | --- |
| Cible | Les cibles peuvent être définies par un service réseau, un ensemble d'adresses, un ensemble d'adresses avec des protocoles et des ports définis ou uniquement des protocoles et des ports définis. Vous pouvez sélectionner l'une des options suivantes :<br>• Non applicable : la règle n'inclut pas les destinations. Par exemple, la règle spécifie uniquement des catégories, ou vous pouvez créer une règle qui autorise toutes les tentatives d'accès d'utilisateurs spécifiques, sauf si la connexion est bloquée par la protection du réseau.<br>• Avec correspondance : la règle s'applique si la destination correspond à une cible spécifiée dans la règle.<br>• Aucune correspondance : la règle s'applique si la destination ne correspond à aucune cible spécifiée dans la règle. |
| Network Services | Vous pouvez sélectionner un ou plusieurs services réseau. |
| Adresse | Ce paramètre indique les adresses IP, les FQDN ou les domaines génériques de l'adresse de destination. Les adresses IP peuvent être au format IPv4 ou IPv6 et peuvent être représentées par une seule adresse IP, une plage d'adresses IP ou une notation CIDR. Par exemple, les formats d'adresse suivants sont pris en charge :<br>• Adresse IP unique : 172.16.10.2<br>• Plage d'adresses IP : de 172.16.10.0 à 172.16.10.255<br>• CIDR : 172.16.10.0/24<br>• FQDN : domaine.exemple.com<br>• Domaine avec caractère générique : *.exemple.com |
| Protocole | Ce paramètre indique si la règle correspond aux tentatives de connexion à l'aide du protocole TCP, UDP ou des deux. Si vous ne sélectionnez aucune option, la valeur par défaut est TCP et UDP sur tous les ports. |
| Port | Ce paramètre indique les ports utilisés pour la destination. Vous pouvez spécifier un port unique ou une plage. |
| Catégorie | Une catégorie définit le type de contenu disponible sur un site. En fonction des informations disponibles, CylanceGATEWAY s'efforce de déterminer la catégorie des sites de destination. Vous pouvez sélectionner l'une des options suivantes :<br>• Non applicable : la règle n'inclut pas les catégories.<br>• Avec correspondance : la règle s'applique si la destination correspond à une catégorie spécifiée dans la règle. Si vous sélectionnez cette option, une liste de sélection de catégories s'affiche.<br>• Aucune correspondance : la règle s'applique si la destination ne correspond à aucune catégorie spécifiée dans la règle. Si vous sélectionnez cette option, une liste de sélection de catégories s'affiche.<br>Pour plus d'informations sur les catégories disponibles pouvant être spécifiées, consultez Catégories de contenu de destination |
| **Conditions** | |

| Élément | Description |
| --- | --- |
| Propriétés utilisateur | Ce paramètre spécifie les utilisateurs, les groupes d'utilisateurs ou les systèmes d'exploitation à inclure dans la règle. Vous pouvez spécifier un nombre illimité d'utilisateurs, de groupes d'utilisateurs et de systèmes d'exploitation, ou une combinaison de chacun d'eux. Lorsque vous cliquez sur la liste déroulante Propriétés utilisateur, sélectionnez la propriété utilisateur dont vous souhaitez spécifier la condition. Vous pouvez sélectionner l'une des options suivantes :<br>• Non applicable : la règle s'applique à tous les utilisateurs, groupes et systèmes d'exploitation.<br>• Avec correspondance : la règle s'applique uniquement aux utilisateurs, groupes et systèmes d'exploitation que vous ajoutez à la règle. Si vous sélectionnez cette option, un champ permettant d'ajouter des propriétés utilisateur s'affiche.<br>• Aucune correspondance : la règle s'applique uniquement aux utilisateurs, groupes et systèmes d'exploitation qui ne sont pas répertoriés dans la règle. Si vous sélectionnez cette option, un champ permettant d'ajouter des propriétés utilisateur s'affiche.<br>Lorsque vous commencez à saisir un nom ou un groupe d'utilisateurs, une liste correspondante de noms d'utilisateurs s'affiche. Lorsque vous spécifiez le système d'exploitation, vous devez le sélectionner dans la liste. Vous pouvez sélectionner l'une des options de système d'exploitation suivantes :<br>• Android<br>• iOS<br>• macOS<br>• Windows<br>Vous pouvez ajouter des lignes pour spécifier le nombre d'utilisateurs, de groupes et de systèmes d'exploitation de votre choix. |
| Risque | Ce paramètre spécifie le niveau de risque acceptable du terminal tel qu'il est configuré dans la stratégie d'évaluation des risques. Pour plus d'informations sur la création d'une politique d'évaluation des risques, consultez Créer une stratégie d'évaluation des risques.<br>• Non applicable : le niveau de risque n'est pas une condition d'accès.<br>• Avec correspondance : le terminal doit être compris dans la plage de niveaux de risque acceptables pour autoriser la connexion. Si vous sélectionnez cette option, vous pouvez sélectionner les niveaux de risque acceptables. Le niveau de risque par défaut est sécurisé (aucun risque). |

## Catégories de contenu de destination

Ces catégories contrôlent le type de contenu auquel les utilisateurs peuvent accéder sur un site disponible. Vous pouvez sélectionner une catégorie entière ou une sous-catégorie que vous souhaitez faire correspondre.

**Adulte**

Contenu réservé aux adultes. Options possibles :

- Adulte
- Alcool et tabac
- Rencontres
- Jeux d'argent
- Nudité
- Langage obscène
- Nudité
- Langage obscène
- Personnel et rencontres
- Pornographie
- Sex Toys
- Maillot de bain et vêtements intimes
- Armes

**Bande passante**

Sites susceptibles d'affecter la vitesse de transfert des données sur votre réseau. Options possibles :

- Téléchargement du logiciel d'application
- Téléchargement des sites
- Communications Internet et téléphonie
- Partage de fichiers multimédias
- Stockage et sauvegarde en ligne
- Domaines en attente
- Domaines en attente
- Poste à poste
- Stockage et sauvegarde sur réseau personnel
- Galerie de photos
- Shareware et Freeware
- Spam
- Diffusion multimédia en continu
- Surveillance
- Hébergement vidéo
- VVOIP

**Informatique et technologies de l'information**

Contenu sur le thème de l'informatique. Options possibles :

- Informations sur l'ordinateur et Internet
- Réseaux de diffusion de contenu
- Sites de numérotation
- DoH
- Adresse électronique
- Technologies de l'information
- Internet
- Portails Internet
- Services en ligne
- Accès à distance
- Contrôle à distance
- Moteurs de recherche
- Technologie et informatique
- Mise à jour des sites
- Redirecteur d'URL
- URL courte
- Sites VPN
- Applications Web
- Collaboration Web
- Hébergement Web
- Infrastructure Web
- E-mail Web

**Intérêt général - entreprise**

Contenu sur le thème de l'entreprise. Options possibles :

- Banque
- Bitcoin
- Commerce
- Commerce et économie
- Applications d'entreprise
- Services financiers
- Organisations à but non lucratif
- Paiement en ligne
- Organisations professionnelles
- Conseils et outils relatifs aux actions

**Intérêt général - personnel**

Contenu sur le thème de l'intérêt personnel. Options possibles :

- Hébergement
- Conseil
- Défense des intérêts
- Arts et culture
- Astrologie
- Blogs et forums d'enchères
- Blogs et wikis
- Dessins animés
- Célébrité
- Cuisine
- Cultes
- Formation et référence
- Établissements d'enseignement
- Divertissement
- Divertissement et arts
- Mode et beauté
- Nourriture et boissons
- Jeux
- Organisations générales
- Santé et médecine
- Maison et jardin
- Humour et satire
- Chasse et pêche
- Institutions
- Enchères en ligne
- Achats en ligne
- Recherche d'emploi
- Enfants
- Style de vie
- Communications mobiles
- Téléphone mobile
- Véhicules motorisés
- Musique
- Actualités
- Occultisme
- Opinion
- Pay to Surf
- Personnel
- Sites personnels et blogs
- Pharmacie
- Philosophie et soutien politique
- Politique
- Salle de presse
- Association professionnelle
- Réseau professionnel
- Informations publiques
- Immobilier
- Loisirs et hobbies
- Référence et recherche
- Religion et philosophie
- Restaurants et nourriture
- Sectes
- Shopping
- Réseaux sociaux
- Société
- Sport
- Suggestions
- Presse
- Formation et outils
- Traduction
- Voyage

**Gouvernement américain**

Contenu sur le thème du gouvernement. Options possibles :

- Gouvernement américain
- Secteur public
- Mention légale
- Armée

**Potentiellement responsable**

Contenu thématique potentiellement responsable. Options possibles :

- Examen de tricherie
- Violation des droits d'auteur
- Criminalité
- Cryptojacking
- Matières dangereuses
- Médicaments
- Extrêmisme
- Fraude
- Haine et discrimination
- Illégal
- Marijuana
- Narcotiques
- Contournement de proxy et anonymiseurs
- Contenu douteux
- Suicide
- Violence

**Productivité**

Sites à thème de contenu susceptibles d'affecter la productivité. Options possibles :

- Publicités et analyses
- Chat et messagerie instantanée
- Contenu insuffisant
- Marketing et publicité
- Application de productivité
- Publicités Web
- Marketing Web et par e-mail

**Risque de sécurité**

Sites qui ne sont pas malveillants, mais qui partagent des informations susceptibles de présenter un risque de sécurité (par exemple, informations relatives à la création de logiciels espions). Options possibles :

| | | |
|---|---|---|
| • Réseaux de bots<br>• Commande et contrôle<br>• Sites Web compromis<br>• DDoS<br>• Tunnel DNS<br>• DNS dynamique | • Sites de vente illégale<br>• Piratage<br>• Logiciels malveillants<br>• Contenu mixte<br>• Hameçonnage<br>• Potentiellement dangereux | • Logiciels potentiellement indésirables<br>• Logiciel espion<br>• Site Web suspect<br>• Marché non autorisé<br>• Warez |

**Inconnu**

Contenu du site qui peut être ou non malveillant. Options possibles :

| | |
|---|---|
| • Divers<br>• Nouveau domaine | • Non résolu<br>• Inconnu |

## Évaluer le niveau de risque d'une destination réseau

Vous pouvez utiliser la console de gestion pour évaluer le niveau de risque et identifier la catégorie et la sous-catégorie d'une destination réseau telle qu'elle serait analysée et déterminée par les services cloud CylanceGATEWAY. Cette fonction fournit des informations sur la manière dont CylanceGATEWAY classerait la destination lorsque l'agent tente d'y accéder. Cela peut vous aider à créer et à mettre à jour vos règles de liste de contrôle d'accès (ACL) pour autoriser ou bloquer une destination. Les destinations qui ne sont pas considérées comme malveillantes renvoient uniquement la catégorie et la sous-catégorie.

**Avant de commencer :** Vous devez disposer du rôle Administrateur pour accéder à cette fonctionnalité dans la console.

1. Dans la barre de menus de la console de gestion, cliquez sur **Protection > Menaces réseau**.
2. Dans le champ de texte, saisissez l'adresse IP de destination, le FQDN ou l'URL.
3. Cliquez sur **Analyser**.

## Configurer la liste de contrôle d'accès

CylanceGATEWAY évalue les connexions existantes vers une destination toutes les cinq minutes. Lors de l'évaluation, CylanceGATEWAY réapplique les règles ACL et la connexion établie peut être déconnectée, si nécessaire. Cela peut se produire si, par exemple, le niveau de risque des utilisateurs a changé ou si la réputation de la destination a été mise à jour depuis l'établissement de la connexion.

**Avant de commencer :** Assurez-vous d'avoir défini votre réseau privé en fonction des besoins de votre entreprise. Pour obtenir des instructions, reportez-vous à la section Définition de votre réseau privé.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Réseau**.
2. Cliquez sur l'onglet **Liste de contrôle d'accès**.
3. Si vous voyez une notification indiquant qu'un ensemble de règles à l'état de brouillon est en cours, cliquez sur l'onglet **Règles de brouillon**.

   Si vous n'avez pas d'ensemble de règles à l'état de brouillon en cours, toute mise à jour que vous effectuez en crée un.
4. Effectuez l'une des actions suivantes :

- Pour rechercher une règle ou une règle provisoire, cliquez sur et sélectionnez une ou plusieurs portées prédéfinies, une condition, puis spécifiez les critères. Cliquez sur la règle dont vous souhaitez afficher les paramètres. Cliquez sur pour réinitialiser la recherche. Pour plus d'informations sur les recherches, consultez Recherche de règles ACL et de services réseau.
- Pour ajouter une nouvelle règle à la fin de la liste, cliquez sur **Ajouter la règle**.
- Pour ajouter une nouvelle règle au-dessus ou au-dessous d'une règle existante, cliquez sur ··· dans la ligne de la règle existante, puis sélectionnez **Ajouter la règle au-dessus** ou **Ajouter la règle au-dessous**.
- Pour copier une règle et l'ajouter au-dessus ou au-dessous d'une règle existante, cliquez sur ··· dans la ligne de la règle existante, puis sélectionnez **Copier la règle au-dessus** ou **Copier la règle au-dessous**.
- Pour modifier une règle existante, cliquez sur le nom de la règle.
- Pour désactiver une règle, cliquez sur dans la ligne de la règle.
- Pour activer une règle, cliquez sur dans la ligne de la règle.
- Pour supprimer une règle, cliquez sur ··· dans la ligne de la règle et sélectionnez **Supprimer la règle**.
- Pour modifier l'ordre des règles, cliquez sur **Organiser** et utilisez les flèches pour déplacer les règles vers le haut ou vers le bas dans la liste.
- Pour ajouter une règle permettant d'autoriser le trafic vers une destination malveillante bloquée dans le cas où les utilisateurs ont besoin d'un accès (par exemple, les utilisateurs qui effectuent une recherche sur les menaces), cliquez sur **Ajouter une règle** avec les paramètres suivants. Cette règle doit être ordonnée avant les autres règles qui autorisent l'accès à une destination.
  - Action : autoriser
  - Option Vérifier les tentatives d'accès par rapport à la protection du réseau : décochez la case.
  - Cible : avec correspondance. Ajoutez l'adresse de destination.
  - Utilisateurs ou groupes : avec correspondance. Ajoutez les utilisateurs ou les groupes qui nécessitent un accès à la destination.

5. Si vous avez choisi d'ajouter ou de modifier une règle, spécifiez les paramètres de la règle ACL et cliquez sur **Enregistrer**.
6. Cliquez sur **Valider les règles** pour appliquer vos modifications à l'ACL.

   Vous pouvez également quitter la page et revenir ultérieurement aux règles de brouillon. Lorsque vous validez un brouillon d'ACL, tous les autres administrateurs disposant d'une liste de règles provisoires sont invités à supprimer leur brouillon obsolète.

# Configurer la protection réseau

Vous pouvez configurer la manière dont CylanceGATEWAY détecte les menaces et réagit à celles-ci de différentes manières. Lorsque vous configurez vos règles de liste de contrôle d'accès (ACL) pour autoriser l'accès aux destinations, CylanceGATEWAY peut toujours empêcher l'utilisateur d'accéder à la destination si une menace potentielle est identifiée. Vous pouvez également contrôler les informations pouvant s'afficher sur l'écran Évènements réseau ou la vue Alertes et celles envoyées à la solution SIEM ou au serveur syslog, si cette fonction est configurée. Pour activer la protection réseau supplémentaire, assurez-vous que le paramètre Vérifier les adresses par rapport à la protection réseau est également sélectionné pour chaque règle ACL. Ce paramètre est activé par défaut.

- Détection de signature : vous pouvez utiliser la détection de signature pour activer la détection approfondie des menaces réseau à l'aide des signatures de la connexion réseau. Lorsque la détection de signature est activée, CylanceGATEWAY bloque automatiquement les connexions qui présentent des menaces si la règle ACL correspond à la destination et vérifie la protection du réseau. Lorsque la détection de signature est désactivée, les menaces sont consignées, mais la connexion n'est pas bloquée. Pour en savoir plus sur une liste de détections et leurs actions, consultez la section Affichage de l'activité réseau. La détection de signature est activée par défaut.

- Protection des destinations : vous pouvez utiliser la réputation de destination pour bloquer les adresses IP et les noms de domaine complets potentiellement malveillants qui correspondent au niveau de risque que vous spécifiez (faible, moyen ou élevé). Lorsque cette option est activée, le niveau de risque par défaut est élevé. CylanceGATEWAY consigne et bloque automatiquement les connexions aux destinations qui correspondent au niveau de risque défini lorsque la destination correspond à la règle ACL et vérifie la protection du réseau. Lorsque la protection de destination est désactivée, les menaces sont consignées, mais la connexion n'est pas bloquée. Pour en savoir plus sur une liste de détections et leurs actions, consultez la section Affichage de l'activité réseau. L'option de réputation de destination est activée par défaut.

  Les niveaux de risque utilisent une combinaison de modèles d'apprentissage automatique (ML) et de base de données statique de réputation d'IP pour déterminer si une destination peut contenir des menaces potentielles.

  - Modèles ML : les modèles ML attribuent un niveau de confiance aux destinations auxquelles vos utilisateurs peuvent accéder. Les modèles ML apprennent en permanence si une destination peut contenir des menaces potentielles.
  - Bases de données de réputation IP : la base de données de réputation IP fournit un niveau de confiance aux adresses IP à partir de flux de réputation IP ouverts et commerciaux. CylanceGATEWAY fait référence aux flux de réputation pour déterminer le niveau de risque d'une adresse IP. CylanceGATEWAY prend en compte le nombre de fournisseurs qui ont reconnu une destination spécifique et la fiabilité des sources avant d'attribuer un niveau de risque (par exemple, si la majorité des sources et des moteurs de réputation IP identifient une destination pour contenir des menaces potentielles, CylanceGATEWAY attribue à la destination un niveau de risque élevé. Pour en savoir plus sur les niveaux de risque, consultez la section Seuil de risque de réputation de destination.

  CylanceGATEWAY applique automatiquement la catégorie Risque dynamique et une sous-catégorie aux détections de réputation IP qui ont été identifiées comme pouvant contenir des menaces malveillantes à l'aide d'une combinaison de modèles d'apprentissage automatique (ML) et de base de données de réputation d'IP. Les bases de données sont en permanence modifiées pour ajouter ou supprimer des entrées de destination. Vous pouvez afficher des métadonnées et des détails supplémentaires pour des évènements réseau catégorisés comme Risque dynamique sur l'écran Évènements réseau. La catégorie Risque dynamique comprend les sous-catégories suivantes :

  | | | |
  |---|---|---|
  | • Balise<br>• Commande et contrôle<br>• Tunnel DNS | • Logiciels malveillants<br>• Hameçonnage<br>• Potentiellement dangereux | • Site Web suspect<br>• Algorithme de génération de domaine (DGA) |

## Seuil de risque de réputation de destination

Vous pouvez indiquer si CylanceGATEWAY doit bloquer l'accès réseau aux destinations potentiellement malveillantes en fonction du seuil minimal que vous avez défini.

| Élément | Description |
|---|---|
| Élevé | Cette catégorie de risque indique qu'il y a plus de 80 % de certitude que la destination est nocive ou malveillante. |
| Moyen | Cette catégorie de risque indique une confiance de 60 à 80 % dans le fait que la destination pourrait être une cybermenace. |
| Faible | Cette catégorie de risque indique un niveau de confiance de 50 à 60 % indiquant que la destination est suspecte ou contient des menaces potentielles. |

## Configurer les paramètres de protection réseau

Vous pouvez spécifier les détections que vous souhaitez activer et afficher sur l'écran Évènements réseau, ainsi que les informations envoyées à la solution SIEM ou au serveur syslog. Vous pouvez également configurer CylanceGATEWAY pour afficher un message aux utilisateurs chaque fois que CylanceGATEWAY bloque une connexion à une destination potentiellement malveillante. Pour obtenir des informations sur les niveaux de risque disponibles, consultez la section Seuil de risque de réputation de destination. Lorsque vous configurez les paramètres de protection réseau, CylanceGATEWAY génèrera des alertes qui s'affichent dans la vue Alertes. Pour plus d'informations, reportez-vous à la section Gestion des alertes sur les services Cylance Endpoint Security.

**Avant de commencer :** Assurez-vous que l'option Vérifier les tentatives d'accès par rapport à la protection du réseau est sélectionnée pour chaque règle ACL. Pour plus d'informations sur les règles ACL, consultez Contrôle de l'accès réseau.

1. Sur la barre de menus, cliquez sur **Paramètres > Réseau**.
2. Cliquez sur l'onglet **Protection du réseau**.
3. Effectuez l'une des opérations suivantes :

| Tâche | Étapes |
| --- | --- |
| Spécifiez les détections que vous souhaitez activer et indiquez si vous souhaitez avertir les utilisateurs lorsqu'elles sont bloquées en raison de détections. | **a.** Cliquez sur l'onglet **Protect**.<br>**b.** Si vous souhaitez afficher un message lorsque CylanceGATEWAY bloque une connexion, sélectionnez **Afficher un message de notification de blocage sur les terminaux**.<br>**c.** Dans le champ **Message**, saisissez le message que vous voulez afficher aux utilisateurs.<br>**d.** Pour activer la détection de signature, sélectionnez **Activer la détection de signature**.<br>Lorsque cette option est activée, des alertes sont générées pour les détections de signature bloquées et s'affichent dans la vue Alertes. Lorsque cette option est désactivée, les alertes ne sont pas générées. Pour plus d'informations, reportez-vous à la section Gestion des alertes sur les services Cylance Endpoint Security.<br>**e.** Pour activer la réputation de destination, sélectionnez **Activer la réputation de destination** et sélectionnez le niveau de risque minimal pour les adresses IP et les FQDN potentiellement malveillants à bloquer.<br>Lorsque cette option est activée, les alertes sont générées et s'affichent dans la vue Alertes en fonction du niveau de risque que vous avez défini. Par exemple, si vous sélectionnez le niveau de risque « Moyen à élevé », les alertes présentant un risque moyen ou élevé s'affichent dans la vue Alertes. Lorsque cette option est désactivée, les alertes CylanceGATEWAY considérées comme présentant un risque élevé sont générées et s'affichent par défaut dans la vue Alertes. |

| Tâche | Étapes |
| --- | --- |
| Spécifiez et contrôlez les détections à afficher dans l'écran Évènements réseau.<br><br>**Remarque :** Si vous activez la confidentialité du trafic et que les tentatives d'accès au réseau répondent à la règle ACL, les tentatives d'accès au réseau ne s'affichent pas dans l'écran Évènements réseau. | **a.** Cliquez sur l'onglet **Rapport**.<br>**b.** Pour afficher les détections de signature pour les évènements réseau autorisés, activez l'option **Afficher les évènements de détection de signature autorisés**. Par défaut, les détections de signature bloquées automatiquement s'affichent dans l'écran Évènements réseau.<br>**c.** Pour afficher les détections de réputation de destination pour les évènements réseau autorisés, activez l'option **Afficher les évènements de réputation de destination autorisés** et sélectionnez le niveau de risque minimal des adresses IP potentiellement malveillantes à afficher. Si cette option est désactivée, les évènements de signature sont capturés comme trafic autorisé normal.<br>**d.** Pour afficher les détections de tunnellisation DNS, activez l'option **Afficher les détections de tunnellisation DNS** et sélectionnez le niveau de risque minimal des menaces en fonction de l'analyse du trafic DNS entre le client et le serveur DNS. Par défaut, le niveau de risque est défini sur Moyen.<br>**e.** Pour afficher les détections du jour zéro, activez l'option **Afficher les détections du jour zéro** et sélectionnez le niveau de risque minimal des destinations malveillantes nouvellement identifiées qui n'ont pas été identifiées précédemment. Par défaut, le niveau de risque est défini sur Moyen. |

| Tâche | Étapes |
| --- | --- |
| Spécifiez et contrôlez les détections à afficher dans la vue Alertes et à envoyer à la solution SIEM ou au serveur syslog, si cette fonction est configurée.<br>**Remarque :** Si vous activez la confidentialité du trafic et que les tentatives d'accès au réseau répondent à la règle ACL, les tentatives d'accès au réseau ne sont pas envoyées à la solution SIEM ou au serveur syslog. | **a.** Cliquez sur l'onglet **Partager**.<br>**b.** Pour envoyer des évènements réseau autorisés ou bloqués et des alertes qui ont des détections de signature, activez l'option **Partager les évènements de détection de signature**. Lorsque cette option est activée, par défaut les détections de signature bloquées sont affichées dans la vue Alertes et envoyées à la solution SIEM ou au serveur syslog. Vous pouvez également sélectionner l'option **Évènements autorisés** pour envoyer les évènements autorisés.<br>**c.** Pour envoyer des évènements réseau et des alertes qui ont des détections de réputation de destination et qui ont été autorisés en fonction du niveau de risque minimal que vous avez défini ou bloqué, activez l'option **Partager les évènements de réputation de destination**. Lorsque cette option est activée, par défaut les évènements de réputation de destination bloqués sont affichés dans la vue Alertes et envoyés à la solution SIEM ou au serveur syslog. Vous pouvez également sélectionner l'option **Évènements autorisés** pour envoyer les évènements autorisés.<br>**d.** Pour envoyer des évènements réseau et des alertes qui ont des détections de tunnellisation DNS en fonction du niveau de risque minimal que vous avez défini, sélectionnez l'option **Partager les détections de tunnellisation DNS**. Par défaut, le niveau de risque est défini sur Moyen.<br>**e.** Pour envoyer des évènements réseau et des alertes qui ont des détections du jour zéro en fonction du niveau de risque minimal que vous avez défini, sélectionnez l'option **Partager les détections du jour zéro**. Par défaut, le niveau de risque est défini sur Moyen.<br>**f.** Pour envoyer des évènements réseau bloqués par des règles ACL, activez l'option **Partager les évènements d'ACL bloqués**. Les évènements ACL bloqués et autorisés ne s'affichent pas dans la vue Alertes. |

**4.** Cliquez sur **Enregistrer**.

# Recherche de règles ACL et de services réseau

Vous pouvez rechercher les règles ACL et les services réseau que vous avez ajoutés à CylanceGATEWAY. CylanceGATEWAY fournit des étendues et des conditions prédéfinies pour vos critères de recherche.

Pour renvoyer des résultats, une recherche s'appuie sur les critères que vous spécifiez dans le champ de recherche pour une étendue et une condition. Par exemple, si vous recherchez dans les règles ACL une règle dont le nom contient « IT » (par exemple, Scope = Name, Condition = Contains et Search Criteria = IT), toutes les règles dont le nom contient « IT » sont renvoyées.

**Remarque :** Vous pouvez effectuer une recherche sur les règles ACL validées ou sur les règles ACL provisoires. Une recherche ne couvre pas les règles ACL validées et provisoires.

Dans les recherches avancées, lorsque plusieurs étendues et critères de recherche sont spécifiés, le moteur de recherche utilise un opérateur AND entre les critères de recherche. Tous les résultats de la recherche contiendront l'ensemble des critères spécifiés. Par exemple, si vous recherchez des services réseau pour un service portant le nom « exemple » et un FQDN « exemple.com » (par exemple,

Scope = Name, Condition = Contains, Search Criteria = Exemple et Scope = FQDN, Condition = Contains, Search Criteria = exemple.com), toutes les règles qui incluent les deux critères sont renvoyées.

La recherche n'est pas sensible à la casse. Par exemple, la recherche « Exemple » ou « exemple » donne les mêmes résultats.

# Utilisation de l'épinglage d'IP source

CylanceGATEWAY vous permet d'obtenir des adresses IP dédiées que vous pouvez utiliser pour l'épinglage IP source. De nombreuses applications SaaS permettent de limiter l'accès aux connexions à partir d'une plage spécifique d'adresses IP de confiance. Votre organisation peut déjà utiliser cette méthode pour limiter l'accès à un locataire d'application SaaS à l'adresse IP utilisée par les terminaux connectés au réseau de votre organisation. Pour les utilisateurs travaillant à distance, cela signifie que vous pouvez sécuriser l'accès entre vos utilisateurs et les applications basées sur le cloud à l'aide de l'épinglage IP source sans avoir à utiliser le VPN de votre entreprise, ce qui peut réduire le trafic sur votre réseau et améliorer les connexions pour les utilisateurs.

Si vous avez activé l'épinglage d'adresses IP source pour CylanceGATEWAY, les paramètres réseau de l'épinglage d'adresses IP source affichent les adresses IP que BlackBerry a attribuées à votre organisation uniquement.

Pour obtenir des adresses IP dédiées, rendez-vous sur support.blackberry.com/community pour lire l'article 96499.

Pour afficher les adresses IP qui vous ont été attribuées, dans la barre de menus, cliquez sur **Paramètres > Réseau**, puis sélectionnez l'onglet **Épinglage IP source**.

# Configurer les options des services Gateway

Vous configurez les stratégies de Gateway Service pour définir des options spécifiques au système d'exploitation qui contrôlent la manière dont les applications peuvent ou non utiliser le tunnel, spécifier si les utilisateurs peuvent accéder aux destinations dont la réputation est mauvaise et demander aux utilisateurs de vérifier leur identité avant de pouvoir établir un tunnel.

## Paramètres de stratégie de service Gateway

Si vous configurez CylanceGATEWAY sur des terminaux activés avec une solution EMM telle que BlackBerry UEM, vous pouvez également spécifier des options dans votre solution EMM qui contrôlent le fonctionnement de CylanceGATEWAY sur les terminaux.

| Élément | Description |
|---|---|
| **Informations générales** | |
| Nom | Il s'agit du nom de la règle. |
| Description | Il s'agit d'une brève description de l'objectif de la règle. |
| **Agent de configuration** | |

| Élément | Description |
| --- | --- |
| Autoriser l'exécution de Gateway uniquement si le terminal est géré par BlackBerry UEM ou Microsoft Intune | Ce paramètre spécifie que les terminaux iOS, Android ou Chromebook doivent être gérés par BlackBerry UEM ou Microsoft Intune avant que les utilisateurs puissent utiliser CylanceGATEWAY.<br>Cette fonctionnalité requiert l'un des éléments suivants :<br>• BlackBerry UEM : le connecteur BlackBerry UEM est ajouté au locataire Cylance Endpoint Security et les applications sont envoyées depuis BlackBerry UEM.<br>• Intune : le connecteur Microsoft Intune est ajouté au locataire Cylance Endpoint Security et vous créez des stratégies de configuration d'applications qui définissent les types de terminaux et les groupes d'utilisateurs Intune auxquels s'applique l'intégration.<br>Pour plus d'informations, reportez-vous à : Connexion de Cylance Endpoint Security aux solutions MDM pour vérifier si les terminaux sont gérés |
| Autoriser Gateway à établir des tunnels uniquement sur les terminaux gérés par MDM sur lesquels Gateway est configurée en tant que VPN géré | Vous pouvez exiger l'inscription d'un terminal dans Mobile Device Management (MDM) pour votre organisation avec CylanceGATEWAY configuré en tant que fournisseur VPN avant que le mode de travail de CylanceGATEWAY ne crée un tunnel sur ce terminal.<br>Cette fonctionnalité est prise en charge sur les terminaux suivants :<br>• Agent CylanceGATEWAY pour macOS 2.7 ou une version ultérieure<br>• Application CylancePROTECT Mobile pour iOS 2.14 ou une version ultérieure |
| Autoriser l'exécution de Gateway uniquement si CylancePROTECT Desktop est également activé sur le terminal. | Ce paramètre nécessite que les utilisateurs aient installé et activé CylancePROTECT Desktop à partir du même locataire. Cette fonctionnalité est prise en charge sur les terminaux suivants :<br>• Terminaux Windows qui exécutent CylanceGATEWAY pour Windows<br>• Terminaux macOS qui exécutent CylancePROTECT Desktop 3.0 ou versions ultérieures ou CylanceGATEWAY pour macOS 2.0.17 ou versions ultérieures. Si vous activez cette fonctionnalité pour les terminaux qui exécutent une version de CylancePROTECT Desktop antérieure à la version 3.0, le tunnel ne fonctionnera peut-être pas comme prévu. |

| Élément | Description |
| --- | --- |
| Mode sans échec | Vous pouvez activer le mode sans échec pour vos utilisateurs. Grâce au mode sans échec, CylanceGATEWAY empêche les applications et les utilisateurs d'accéder à des destinations potentiellement malveillantes et met en application une stratégie d'utilisation acceptable (SUA) en interceptant les demandes DNS. Les services cloud CylanceGATEWAY évaluent chaque requête DNS par rapport aux règles ACL configurées et aux paramètres de protection réseau (par exemple, Tunnellisation DNS et détections Du jour zéro telles que Algorithme de génération de domaine (DGA), Hameçonnage et Programmes malveillants), puis demandent à l'agent d'autoriser ou de bloquer la demande en temps réel. En cas d'autorisation, la demande DNS est exécutée normalement sur le réseau porteur. Dans le cas contraire, l'agent CylanceGATEWAY remplace la réponse normale et empêche l'accès.<br><br>Lorsqu'il est activé, le mode sans échec prend automatiquement effet lorsque le mode de travail est désactivé. Lorsqu'il est activé pour les terminaux Windows, l'agent est réduit dans la barre d'état système lors de son lancement. L'activation du mode sans échec n'empêche pas les utilisateurs d'ouvrir l'agent, ni d'activer ou de désactiver le mode de travail (si la stratégie des utilisateurs autorise de telles opérations).<br><br>Les évènements du mode sans échec apparaissent sur l'écran Évènements CylanceGATEWAY et la vue Alertes, puis sont envoyés vers la solution SIEM ou le serveur syslog, si cette fonction est configurée.<br><br>**Remarque :** Lorsqu'il est activé, le mode sans échec protège l'ensemble du trafic DNS qui n'utilise pas le tunnel CylanceGATEWAY (par exemple, autoriser Gateway à établir des tunnels uniquement sur les terminaux gérés par MDM sur lesquels Gateway est configurée en tant que VPN géré, tunnel par application ou tunnellisation fractionnée).<br><br>Cette fonctionnalité est prise en charge sur les terminaux suivants :<br>• Agent CylanceGATEWAY pour Windows 2.8 ou une version ultérieure.<br>• Agent CylanceGATEWAY pour macOS 2.7 ou une version ultérieure.<br><br>**Remarque :** Cette fonctionnalité n'est pas prise en charge dans les environnements qui utilisent des protocoles DNS sécurisés avec DoT (DNS sur TLS) et DoH (DNS sur HTTPS). Les requêtes DNS envoyées à l'aide de DoT ou DoH ne peuvent pas être visualisées par CylanceGATEWAY.<br><br>**Mode sans échec et agent CylanceGATEWAY pour macOS** : sous macOS, l'agent CylanceGATEWAY utilise une extension système pour implémenter le mode sans échec. Si vous ajoutez l'extension système « P7E3XMAM8G:com.blackberry.big3.gatewayfilter » à une liste autorisée, elle peut se charger automatiquement sans intervention de l'utilisateur lorsque l'agent CylanceGATEWAY est activé. Sinon, demandez à vos utilisateurs d'autoriser l'extension système CylanceGATEWAY lorsqu'ils y sont invités au cours de l'activation. Pour en savoir plus sur l'ajout d'une extension système à une liste autorisée, consultez la documentation de votre macOS. Pour obtenir plus d'instructions sur l'activation de l'agent CylanceGATEWAY en vue d'utiliser le mode sans échec, consultez la section Activer le mode sans échec dans l'agent CylanceGATEWAY du guide de l'utilisateur.<br><br>**Mode sans échec et VPN tiers** : si votre environnement est configuré pour utiliser le mode sans échec et un VPN tiers, vous devez vérifier et, si nécessaire, ajuster les paramètres DNS du VPN pour vous assurer que les paramètres DNS acheminent uniquement les requêtes DNS pour le trafic défini pour utiliser le tunnel VPN. Si vous activez le mode sans échec et que les paramètres DNS du VPN ne sont pas examinés, le VPN risque de ne pas fonctionner comme prévu. Par défaut, la configuration de nombreux VPN consiste à acheminer tout le trafic DNS via le tunnel VPN lorsqu'il est actif. |

| Élément | Description |
| --- | --- |
| Appliquer le paramètre Démarrer CylanceGATEWAY lorsque je me connecte | Ce paramètre détermine s'il convient de forcer le démarrage automatique de l'agent CylanceGATEWAY sur les terminaux macOS ou Windows lorsque les utilisateurs se connectent. Ce paramètre de stratégie remplace le paramètre Démarrer CylanceGATEWAY lorsque je me connecte de l'agent.<br>BlackBerry vous recommande d'activer cette option dans la stratégie de service Gateway.<br>Cette fonctionnalité est prise en charge sur les terminaux suivants :<br>• Agent CylanceGATEWAY pour macOS 2.7 ou une version ultérieure<br>• Agent CylanceGATEWAY pour Windows 2.7 ou une version ultérieure |
| Démarrer automatiquement CylanceGATEWAY lorsque l'utilisateur se connecte | Ce paramètre démarre automatiquement l'agent CylanceGATEWAY lorsque les utilisateurs se connectent au terminal, mais les utilisateurs peuvent toujours arrêter l'agent manuellement. Lorsque vous activez à la fois ce paramètre et l'option Activer le mode de travail automatiquement pour les terminaux Windows, l'agent est réduit dans la barre d'état système lorsqu'il démarre.<br>Ce paramètre n'est valide que si le paramètre Appliquer le paramètre Démarrer CylanceGATEWAY lorsque je me connecte est activé. |
| Appliquer le paramètre « Activer le Mode travail automatiquement » | Ce paramètre détermine s'il convient de forcer le démarrage automatique de l'agent CylanceGATEWAY sur les terminaux macOS ou Windows pour activer le mode de travail automatiquement au démarrage de l'agent. Ce paramètre de stratégie remplace le paramètre Activer le mode de travail automatiquement de l'agent.<br>Cette fonctionnalité est prise en charge sur les terminaux suivants :<br>• Agent CylanceGATEWAY pour macOS 2.7 ou une version ultérieure.<br>• Agent CylanceGATEWAY pour Windows 2.7 ou une version ultérieure |
| Activer le mode de travail automatiquement | Ce paramètre active automatiquement le mode de travail au démarrage de l'agent CylanceGATEWAY, mais les utilisateurs peuvent toujours activer et désactiver manuellement le mode de travail après le démarrage de l'agent. Lorsque vous activez à la fois ce paramètre et l'option Démarrer automatiquement CylanceGATEWAY lorsque l'utilisateur se connecte pour les terminaux Windows, l'agent est réduit dans la barre d'état système lorsqu'il démarre.<br>Ce paramètre n'est valide que si le paramètre Appliquer le paramètre Activer le mode de travail automatiquement est activé. |
| **Utilisation de tunnel** | |

| Élément | Description |
| --- | --- |
| Tunnel par application | Ce paramètre spécifie les applications pouvant envoyer des données aux services cloud CylanceGATEWAY via le tunnel. Vous pouvez configurer un tunnel par application avec une liste d'applications autorisées ou d'applications restreintes. Par exemple, si vous sélectionnez l'option Applications autorisées et que vous spécifiez des applications pouvant utiliser le tunnel, puis que vous modifiez l'option sur Applications restreintes, les applications répertoriées ne peuvent pas utiliser le tunnel.<br><br>Options possibles :<br><br>• Sélectionnez **Applications autorisées** pour spécifier les applications qui utilisent le tunnel. Aucune autre application ne peut utiliser le tunnel. Les applications système et le DNS Windows utilisent toujours le tunnel. Si vous sélectionnez cette option, toutes les règles ACL ou stratégies de contrôle d'accès réseau définies sont appliquées. Pour plus d'informations sur les règles ACL et les stratégies de contrôle d'accès réseau, consultez Contrôler l'accès réseau.<br>• Sélectionnez **Applications interdites** pour spécifier les applications ne pouvant pas utiliser le tunnel. Toutes les autres applications peuvent utiliser le tunnel.<br>• Cliquez sur ⊕ et saisissez le chemin d'accès complet ou incluez un caractère générique dans le chemin d'accès aux applications de bureau, ou ajoutez le nom de famille du package (NFP) Windows pour les applications de la boutique. Vous pouvez spécifier un maximum combiné de 200 chemins d'accès aux applications ou NFP.<br><br>Lorsque vous incluez un caractère générique dans le chemin d'accès, tenez compte des points suivants :<br><br>• Vous ne pouvez inclure qu'un seul caractère générique par chemin d'accès. Le format pris en charge est le suivant : *\ (par exemple, %ProgramFiles%*Folder_Name***Application_Name*.exe)<br>• Les caractères génériques ne sont pas pris en charge dans les cas suivants :<br><br>• Vous les utilisez à la place de variables d'environnement<br>• Vous les utilisez à la place de répertoires racines dans le chemin d'accès<br>• Vous les utilisez dans les noms de répertoire partiels (par exemple, « C:\Win*\notepad.exe »)<br>• Vous les utilisez dans les noms de fichiers exécutables (par exemple, « C:\Windows*.exe »)<br><br>Les caractères génériques sont pris en charge sur les terminaux Windows qui exécutent l'agent CylanceGATEWAY pour Windows 2.7 ou une version ultérieure.<br><br>Cette fonctionnalité est prise en charge sur les terminaux suivants :<br><br>• CylanceGATEWAY pour Windows 2.0.0.13 ou une version ultérieure.<br>• Utilisateurs des terminaux Android ou Chromebook qui exécutent l'application CylancePROTECT Mobile. |

| Élément | Description |
| --- | --- |
| Forcer les applications à utiliser le tunnel | Ce paramètre nécessite que toutes les connexions sans boucle utilisent le tunnel. Si vous sélectionnez cette option et que la tunnellisation fractionnée est activée, tout le trafic utilisera le tunnel. Sur les terminaux Windows, si vous sélectionnez cette option et que la tunnellisation fractionnée est activée, les connexions qui n'utilisent pas le tunnel risquent de ne pas fonctionner comme prévu. Cette fonctionnalité est prise en charge sur les terminaux suivants :<br>• Terminaux non gérés macOS qui exécutent macOS 10.15 ou versions ultérieures et CylanceGATEWAY pour macOS 2.0.17 ou versions ultérieures.<br>• Terminaux non gérés iOS qui exécutent iOS 14.0 ou versions ultérieures et CylancePROTECT Mobile 2.4.0.1731 ou versions ultérieures.<br>• Terminaux Windows qui exécutent CylanceGATEWAY pour Windows |
| Autoriser les applications à utiliser le réseau local | Ce paramètre permet aux applications forcées d'utiliser le tunnel d'atteindre les destinations du réseau local. Cette fonctionnalité est prise en charge sur les terminaux suivants :<br>• Terminaux non gérés macOS qui exécutent macOS 10.15 ou versions ultérieures et CylanceGATEWAY pour macOS 2.0.17 ou versions ultérieures.<br>• Terminaux non gérés iOS qui exécutent iOS 14.2 ou versions ultérieures et CylancePROTECT Mobile 2.4.0.1731 ou versions ultérieures.<br>• Terminaux Windows qui exécutent CylanceGATEWAY pour Windows 2.5 ou versions ultérieures.<br>Ce paramètre n'est valide que si l'option « Forcer les applications à utiliser le tunnel » est activée. |
| Bloquer le trafic réseau des applications limitées | Ce paramètre empêche toutes les connexions réseau sans boucle des applications qui ne peuvent pas utiliser le tunnel. Si vous ne sélectionnez pas ce paramètre, les applications interdites peuvent utiliser la connexion réseau par défaut. Cette fonctionnalité est prise en charge sur les terminaux qui exécutent CylanceGATEWAY pour l'agent de Windows. |
| Autoriser les autres utilisateurs Windows à utiliser le tunnel | Ce paramètre permet à tous les utilisateurs qui utilisent le même terminal Windows d'utiliser le tunnel. Si vous sélectionnez cette option, tous les critères de tunnel par application s'appliquent. Si vous ne sélectionnez pas cette option, les applications exécutées par d'autres utilisateurs Windows sont traitées comme des applications interdites. |
| Autoriser les connexions entrantes | Ce paramètre autorise les connexions TCP entrantes et les flux UDP à partir d'interfaces sans tunnel et sans boucle. CylanceGATEWAY n'achemine jamais les connexions entrantes à travers le tunnel. Cette fonctionnalité est prise en charge sur les terminaux qui exécutent CylanceGATEWAY pour l'agent de Windows. |
| **Réauthentification du tunnel** | |

| Élément | Description |
| --- | --- |
| Réauthentification du tunnel | Ce paramètre spécifie la fréquence à laquelle les utilisateurs doivent s'authentifier avant d'établir un tunnel.<br>Lorsque vous activez cette fonctionnalité, BlackBerry vous recommande de définir l'option Autoriser la réutilisation de l'authentification afin de spécifier la période après laquelle les utilisateurs doivent s'authentifier à nouveau.<br>Cette fonctionnalité est prise en charge sur les terminaux suivants :<br>• CylanceGATEWAY pour macOS 2.5 ou une version ultérieure.<br>• CylanceGATEWAY pour Windows 2.5 ou une version ultérieure. |
| Autoriser la réutilisation de l'authentification | Lorsqu'il est activé, ce paramètre spécifie une période de réutilisation après laquelle les utilisateurs qui se sont authentifiés et ont établi un tunnel doivent s'authentifier à nouveau. La période de réutilisation peut être définie entre 5 minutes et 365 jours à compter de la dernière authentification. Par exemple, si vous définissez la période de réinitialisation sur 10 jours, les utilisateurs doivent s'authentifier à nouveau 10 jours après leur première authentification avant de pouvoir établir un tunnel. Par défaut, ce paramètre est désactivé.<br>**Remarque :** Si vous n'activez pas l'option Autoriser la réutilisation de l'authentification et spécifiez une période de réutilisation, les utilisateurs doivent s'authentifier à chaque fois qu'ils établissent un tunnel.<br>Ce paramètre n'est valide que si « Réauthentification du tunnel » est activée. |
| Période de grâce | Ce paramètre permet aux utilisateurs de se reconnecter au tunnel sans s'authentifier si la connexion au tunnel est établie dans les 2 minutes suivant la déconnexion. Par défaut, cette option est activée lorsque vous activez la réauthentification du tunnel.<br>Ce paramètre n'est valide que si « Réauthentification du tunnel » est activée. |
| **Tunnellisation fractionnée** | |

| Élément | Description |
| --- | --- |
| Tunnellisation fractionnée | Ce paramètre permet au trafic vers les destinations publiques de contourner CylanceGATEWAY. Vous pouvez saisir des adresses CIDR ou des FQDN pour les destinations qui doivent traverser le tunnel. Pour améliorer l'expérience utilisateur, la console de gestion actualise régulièrement le FQDN en fonction de la résolution d'adresse IP.<br><br>**Remarque :** Les adresses FQDN ne prennent pas en charge les caractères génériques.<br><br>Si vous activez la tunnellisation fractionnée, les connexions aux destinations publiques autorisées contournent le tunnel et les services cloud CylanceGATEWAY, sauf si vous spécifiez que les connexions à la destination doivent utiliser le tunnel. Si vous activez la tunnellisation fractionnée sans le DNS fractionné, toutes les requêtes DNS sont évaluées par rapport aux règles ACL configurées et les contrôles d'accès au réseau sont appliqués avant que le trafic ne soit acheminé vers la destination publique. Vous pouvez saisir des adresses CIDR ou des FQDN pour les destinations qui doivent traverser le tunnel. Si vous utilisez l' Ipinglage d'IP source, toutes les destinations configurées pour l'épinglage d'IP source doivent utiliser le tunnel.<br><br>Si vous apportez des modifications aux paramètres de tunnellisation ou aux connexions entrantes, les utilisateurs doivent désactiver puis activer le mode Travail dans l'agent CylanceGATEWAY installé sur les terminaux Windows et macOS ou dans l'application CylancePROTECT Mobile sur les terminaux iOS, Android et Chromebook 64 bits pour que les modifications prennent effet. |
| DNS fractionné | Lorsqu'il est activé, ce paramètre permet d'effectuer des recherches DNS pour les domaines répertoriés dans la configuration Réseau privé > DNS > Zone de recherche directe via le tunnel où les contrôles d'accès au réseau sont appliqués. Toutes les autres recherches DNS sont effectuées à l'aide du DNS local. Si vous avez activé le mode sans échec, le trafic DNS qui n'utilise pas le tunnel Gateway est protégé par le mode sans échec. Le paramètre DNS fractionné est désactivé par défaut.<br><br>Les terminaux Android et Chromebook 64 bits ne prennent pas en charge le tunnel DNS fractionné et utilisent le tunnel où les contrôles d'accès sont appliqués.<br><br>Ce paramètre n'est valide que si l'option Tunnellisation fractionnée est activée. |

## Configurer les options des services Gateway

1. Sur la barre de menus, cliquez sur **Stratégies > Stratégie d'utilisateur**.
2. Cliquez sur l'onglet **Service Gateway**.
3. Cliquez sur l'onglet **Ajouter une stratégie**.
4. Spécifiez les paramètres de stratégie du service Gateway.
5. Cliquez sur **Ajouter**.
6. Si vous apportez des modifications aux paramètres de tunnellisation ou aux connexions entrantes, les utilisateurs doivent désactiver puis activer le mode Travail dans l'agent CylanceGATEWAY installé sur les terminaux Windows et macOS ou dans l'application CylancePROTECT Mobile sur les terminaux iOS, Android et Chromebook pour que les modifications prennent effet.

**À la fin :**

- Attribuer la stratégie à des utilisateurs et des groupes
- Si nécessaire, classez les stratégies.

## Spécification de l'utilisation du tunnel CylanceGATEWAY par les terminaux activés avec une solution EMM

CylanceGATEWAY est une solution d'accès réseau zéro confiance (ZTNA) assistée par l'intelligence artificielle (IA), native dans le cloud. Lorsque CylanceGATEWAY est activé sur un terminal, ce dernier reconnaît CylanceGATEWAY comme fournisseur VPN qui établit un profil d'accès réseau zéro confiance. Si vous avez activé des terminaux à l'aide de BlackBerry UEM ou d'une autre solution EMM, les options VPN que vous définissez dans votre solution EMM peuvent affecter le fonctionnement de CylanceGATEWAY sur ces terminaux.

Pour les terminaux iOS, vous pouvez utiliser votre solution BlackBerry UEM ou d'une autre solution EMM pour configurer un VPN par application afin de désigner les applications qui envoient des données via le tunnel CylanceGATEWAY. Les terminaux doivent être activés pour permettre la gestion des VPN et des applications. Pour en savoir plus, consultez les sections suivantes :

- Spécifier quelles applications utilisent CylanceGATEWAY sur les terminaux iOS
- Spécifier quelles applications utilisent CylanceGATEWAY sur les terminaux iOS dans un environnement Microsoft Intune

Pour les terminaux Android, vous pouvez utiliser BlackBerry UEM ou une autre solution EMM pour forcer CylanceGATEWAY l'activation permanente et empêcher les utilisateurs de modifier la configuration VPN dans le profil professionnel. Pour en savoir plus, consultez les sections suivantes :

- Spécifier les options CylanceGATEWAY sur des terminaux Android Enterprise
- Spécifier les options CylanceGATEWAY sur les terminaux Android Enterprise de votre environnement Microsoft Intune

### Spécifier quelles applications utilisent CylanceGATEWAY sur les terminaux iOS

Pour les terminaux iOS, si votre organisation gère des terminaux à l'aide d'une solution EMM qui prend en charge la configuration du VPN par application, vous pouvez configurer les terminaux pour qu'ils se reconnaissent CylanceGATEWAY en tant que fournisseur VPN et configurer le VPN par application pour spécifier quelles applications envoient des données via le tunnel CylanceGATEWAY.

Pour configurer des options de tunnel par application, vous devez disposer d'autorisations pour la gestion VPN et la gestion des applications sur les terminaux iOS activés à l'aide de votre solution EMM. Pour spécifier les applications qui utilisent le tunnel CylanceGATEWAY dans BlackBerry UEM, procédez comme suit :

1. Dans la console de gestion UEM, ajoutez les applications auxquelles vous souhaitez que des données soient envoyées de CylanceGATEWAY à UEM et attribuez-les aux utilisateurs.

   Seules les applications attribuées aux utilisateurs utilisent le tunnel CylanceGATEWAY. N'attribuez pas le navigateur par défaut ou l'application CylancePROTECT Mobile aux utilisateurs, sinon le terminal ne pourra pas établir de tunnel avec CylanceGATEWAY.

   Pour les terminaux avec les types d'activation Confidentialité de l'utilisateur et Confidentialité de l'utilisateur - Inscription de l'utilisateur, seules les applications internes attribuées et les applications sous licence via Apple le programme d'achat en volume utilisent le tunnel.
2. Créez un profil d'activation qui attribue l'un des types d'activation suivants :
   - Contrôles MDM
   - Confidentialité de l'utilisateur - Inscription de l'utilisateur
   - Confidentialité de l'utilisateur avec la gestion VPN et la gestion des applications activées

3. Créez un profil VPN et incluez les paramètres suivants :

| Paramètre | Description |
|---|---|
| Type de connexion | Personnalisé(e) |
| ID d'offre VPN | com.blackberry.protect |
| Serveur | Ce paramètre spécifie le FQDN ou l'adresse IP d'un serveur VPN. La valeur doit être 127.0.0.1. |
| Type d'authentification | Mot de passe |
| Mot de passe | Laissez ce champ vide |
| Activer un VPN par application | Sélectionné |
| Paramètres de domaine | Spécifiez les domaines qui peuvent établir une connexion via le tunnel CylanceGATEWAY. Si vous spécifiez un domaine, les applications attribuées utilisent le tunnel uniquement pour les connexions au domaine spécifié. Vous pouvez spécifier des domaines pour Safari, Calendrier, Contacts, Messagerie, et les domaines répertoriés dans le fichier d'association apple-app-site. Vous pouvez également spécifier des domaines qui n'utilisent jamais le tunnel.<br>Pour les terminaux avec les types d'activation Confidentialité de l'utilisateur et Confidentialité de l'utilisateur - Inscription de l'utilisateur, si vous spécifiez un domaine qui n'est pas un enfant du domaine racine spécifié dans le champ **Serveur**, le terminal ignore l'intégralité du profil VPN, et pas seulement le domaine non valide. |
| Autoriser la connexion automatique des applications | Sélectionnez cette option pour indiquer que l'application peut démarrer la connexion automatiquement.<br>**Remarque :** Les connexions via le tunnel CylanceGATEWAY peuvent démarrer uniquement si CylanceGATEWAY est activé dans l'application CylancePROTECT Mobile sur le terminal. |
| Tunnellisation du trafic | Couche IP |

4. Attribuez des profils aux utilisateurs et demandez-leur d'activer les terminaux.

#### Spécifier quelles applications utilisent CylanceGATEWAY sur les terminaux iOS dans un environnement Microsoft Intune

Vous pouvez configurer les terminaux iOS pour qu'ils reconnaissent CylanceGATEWAY en tant que fournisseur VPN et configurent un VPN par application en vue de spécifier les applications qui envoient des données via le tunnel CylanceGATEWAY. Dans Microsoft Intune, vous pouvez configurer les paramètres ayant une incidence sur CylanceGATEWAY.

Pour configurer des options de tunnel par application, vous devez disposer d'autorisations de gestion des VPN et de gestion des applications sur les terminaux iOS activés à l'aide de Intune. Pour spécifier les applications qui utilisent le tunnel CylanceGATEWAY dans Intune, procédez comme suit :

1. Dans le centre d'administration de Microsoft Intune, ajoutez les applications auxquelles vous souhaitez que des données soient envoyées de CylanceGATEWAY à Intuneet attribuez-les aux utilisateurs.

Seules les applications attribuées aux utilisateurs utilisent le tunnel CylanceGATEWAY. N'attribuez pas le navigateur par défaut ou l'application CylancePROTECT Mobile aux utilisateurs, auquel cas le terminal ne pourra pas établir de tunnel avec CylanceGATEWAY.

2. Créez un profil VPN et incluez les paramètres suivants. Pour en savoir plus sur les paramètres de iOS et d'iPadOS, consultez la section Ajouter des paramètres VPN sur les terminaux iOS et iPadOS.

| Paramètre | Description |
|---|---|
| Type de connexion | VPN personnalisé |
| Adresse du serveur VPN | La valeur doit être 127.0.0.1. La valeur n'est pas utilisée par CylanceGATEWAY. |
| Mode d'authentification | Nom d'utilisateur et mot de passe |
| Tunnellisation fractionnée | Désactiver |
| Identifiant VPN | Pour les terminaux iOS, saisissez com.blackberry.protect<br>Pour les terminaux macOS, saisissez com.blackberry.big |
| | • Clé : *clé*<br>• Valeur : *valeur*<br>Microsoft Intune nécessite un attribut personnalisé. CylanceGATEWAY n'utilise pas ce paramètre. Vous pouvez saisir n'importe quel attribut. |
| VPN automatique | VPN par application |
| Type de fournisseur | Tunnel de paquets |
| URL Safari | Spécifiez les domaines qui peuvent établir une connexion via le tunnel CylanceGATEWAY. Intune ne prend pas en charge les caractères génériques dans les domaines, car ceux-ci sont implicites. Par exemple, si vous saisissez « org », « *.org » est implicite.<br>**Remarque :** Les connexions via le tunnel CylanceGATEWAY peuvent démarrer uniquement si CylanceGATEWAY est activé dans l'application CylancePROTECT Mobile sur le terminal.<br>Si vous spécifiez blackberry.com comme VPN Safari géré, il est impossible d'activer les applications CylancePROTECT Mobile nouvellement activées. |

3. Si nécessaire, demandez aux utilisateurs d'activer l'application CylancePROTECT Mobile.

#### Spécifier les options CylanceGATEWAY sur des terminaux Android Enterprise

Dans le cas de terminaux Android, vous pouvez spécifier les applications qui envoient des données via le tunnel CylanceGATEWAY à l'aide de la stratégie de service CylanceGATEWAY. Si votre organisation gère des terminaux Android Enterprise à l'aide d'une solution EMM telle que BlackBerry UEM, vous pouvez configurer les paramètres de votre fournisseur EMM qui affectent CylanceGATEWAY.

Vous pouvez utiliser la stratégie informatique dans BlackBerry UEM pour spécifier si CylanceGATEWAY est toujours activé sur les terminaux et si les utilisateurs peuvent modifier les configurations VPN dans le profil

professionnel sur le terminal. Pour plus d'informations sur les règles de stratégie informatique UEM, téléchargez la Référence de stratégie informatique UEM.

1. Dans la console de gestion UEM, créez ou modifiez une stratégie informatique.
2. Effectuez l'une des actions suivantes :
   a) Pour forcer l'activation permanente de CylanceGATEWAY, définissez les règles de stratégie informatique suivantes pour le profil professionnel Android.

| règle de stratégie informatique | Description |
|---|---|
| Forcer la disponibilité du VPN | Sélectionné |
| Utiliser BlackBerry Secure Connect Plus pour la connexion VPN | Non sélectionné |
| ID de package d'application VPN | com.blackberry.protect |
| Forcer les applications professionnelles à utiliser VPN uniquement | Non sélectionné Si cette option est sélectionnée, l'application CylancePROTECT Mobile ne peut pas être activée sur le terminal. |
| Applications professionnelles exemptées du VPN | Si la règle « Forcer les applications professionnelles à utiliser VPN uniquement » est sélectionnée,<br>• vous devez saisir `com.android.chrome` pour autoriser le navigateur Chrome à accéder au réseau et activer l'application CylancePROTECT Mobile sur le terminal avant que le VPN ne soit connecté. Cette règle s'applique aux terminaux exécutant Android OS 10.0.0 ou versions ultérieures.<br>• Si vous saisissez `com.android.protect`, l'application CylancePROTECT Mobile peut accéder au réseau sans utiliser le VPN uniquement lorsque le VPN n'est pas connecté. |

   b) Pour autoriser les terminaux à envoyer des données via le tunnel CylanceGATEWAY si l'option **Forcer la disponibilité du VPN** n'est pas sélectionnée, sélectionnez **Autoriser le VPN configuré par l'utilisateur dans l'espace Travail**.

   Si aucune des options **Forcer la disponibilité du VPN** et **Autoriser le VPN configuré par l'utilisateur dans l'espace Travail** ne sont sélectionnées, le terminal n'autorise pas les applications professionnelles à envoyer des données via le tunnel.
3. Attribuez la stratégie informatique à des utilisateurs.

#### Spécifier les options CylanceGATEWAY sur des terminaux Chromebook

Dans le cas de terminaux Chromebook 64 bits, vous pouvez spécifier les applications qui envoient des données via le tunnel CylanceGATEWAY à l'aide de la stratégie de service CylanceGATEWAY. Si votre organisation gère des terminaux d'entreprise Chrome OS à l'aide d'un domaine Google, vous pouvez forcer CylanceGATEWAY à toujours être activé et empêcher les utilisateurs de modifier la configuration VPN dans l'application CylancePROTECT Mobile. Pour obtenir des instructions, rendez-vous sur https://support.google.com/ et lisez « Configurer des réseaux privés virtuels (application VPN Android) ». Vous pouvez également étendre la gestion des terminaux d'entreprise Chromebook à votre fournisseur EMM, par exemple BlackBerry UEM. Pour plus d'informations, consultez la section Étendre la gestion des terminaux Chrome OS à BlackBerry UEM.

#### Spécifier les options CylanceGATEWAY sur les terminaux Android Enterprise de votre environnement Microsoft Intune

Dans le cas de terminaux Android, vous pouvez spécifier les applications qui envoient des données via le tunnel CylanceGATEWAY à l'aide de la stratégie Gateway. Dans Microsoft Intune, vous pouvez configurer les paramètres ayant une incidence sur CylanceGATEWAY.

Vous pouvez utiliser le profil de configuration pour déterminer si CylanceGATEWAY est toujours activé sur les terminaux et si les utilisateurs peuvent modifier les configurations VPN dans le profil sur le terminal. Pour en savoir plus sur les paramètres du profil de configuration, consultez la section Paramètres du terminal Android Enterprise pour configurer le VPN.

1. Dans le centre d'administration de Microsoft Intune, créez un profil de configuration. Définissez les paramètres suivants :
   - Plateforme : Android Enterprise
   - Type de profil : restrictions de terminal
2. Définissez les règles suivantes pour le profil de configuration.

| Paramètre | Description |
|---|---|
| VPN permanent | Activer |
| Client VPN | Personnalisé(e) |
| ID de package | com.blackberry.protect |
| Mode Verrouiller | Non configuré. Si cette option est sélectionnée, l'application CylancePROTECT Mobile risque de ne pas s'activer. |

3. Attribuez le profil de configuration aux utilisateurs.
4. Attribuez l'application CylancePROTECT Mobile aux utilisateurs.

# Connexion de Cylance Endpoint Security aux solutions MDM pour vérifier si les terminaux sont gérés

Vous pouvez connecter Cylance Endpoint Security à BlackBerry UEM ou Microsoft Intune pour que Cylance Endpoint Security puisse vérifier si les terminaux iOS et Android sont gérés.

Après avoir établi la connexion à UEM, configurez les terminaux iOS et Android, les utilisateurs et les groupes auxquels l'intégration s'applique. Pour UEM, assurez-vous que les utilisateurs sont activés avec un type d'activation pris en charge et gérez la distribution de l'application CylancePROTECT Mobile à l'aide des fonctionnalités de gestion des utilisateurs et des groupes disponibles dans la console de gestion UEM.

Notez que vous devez déployer l'application CylancePROTECT Mobile à partir de l'instance BlackBerry UEM sur tous les terminaux gérés par BlackBerry UEM avec lesquels vous utilisez cette fonctionnalité.

Dans le cadre de l'intégration de Intune, lorsque vous connectez Cylance Endpoint Security à Intune, vous créez des stratégies de configuration d'applications qui définissent les types de terminaux et les groupes d'utilisateurs Intune auxquels s'applique l'intégration. Notez que tous les terminaux gérés par Intune sur lesquels vous souhaitez utiliser cette fonctionnalité doivent être inclus dans une stratégie de configuration d'applications dans la console Cylance via le menu Actifs > Groupes d'utilisateurs.

Dans la console Cylance, vous créez et attribuez la stratégie de service Gateway qui permet à Gateway de s'exécuter uniquement si le terminal est géré par BlackBerry UEM ou Intune. Lorsque l'utilisateur tente d'accéder

à une destination réseau sur un terminal géré par MDM, si la destination est autorisée, le trafic réseau est envoyé via le tunnel sécurisé.

Pour connecter Cylance Endpoint Security à BlackBerry UEM, procédez comme suit.

| Étape | Action |
|---|---|
| 1 | Examinez les conditions préalables. |
| 2 | Établissez une liaison avec votre annuaire d'entreprise.<br>• Dans Cylance Endpoint Security, consultez la section Association à votre annuaire d'entreprise.<br>• Dans BlackBerry UEM, consultez la section Connexion de vos annuaires d'entreprise. |
| 3 | Installez et configurez BlackBerry Connectivity Node.<br>• Dans Cylance Endpoint Security, consultez la section Installation ou mise à niveau de BlackBerry Connectivity Node.<br>• Dans BlackBerry UEM, consultez la section Installer une instance BlackBerry Connectivity Node. |
| 4 | Ajouter un connecteur BlackBerry UEM. |
| 5 | Utiliser BlackBerry UEM pour installer l'application CylancePROTECT Mobile sur des terminaux. |

Pour connecter Cylance Endpoint Security à Intune, procédez comme suit :

| Étape | Action |
|---|---|
| 1 | Examinez les conditions préalables. |
| 2 | Connecter Cylance Endpoint Security à Intune. |

### Conditions préalables : Vérifier que les terminaux sont gérés par MDM

- BlackBerry UEM
  - BlackBerry UEM Cloud ou UEM 12.15 ou une version ultérieure sur site est prise en charge.
  - Assurez-vous de disposer d'un ID SRP et d'une clé d'authentification BlackBerry UEM valides pour vos instances BlackBerry UEM Cloud et BlackBerry UEM. Vous pouvez afficher les ID SRP et les clés d'authentification de vos instances UEM dans votre espace *my*Account, sous Organisation > Services > UEM.
  - Le locataire Cylance Endpoint Security et le domaine UEM de votre organisation doivent avoir le même ID d'organisation.
  - Pour les environnements BlackBerry UEM sur site, vous devez autoriser les connexions à partir du connecteur BlackBerry UEM. Si vous n'autorisez pas les connexions à partir du connecteur BlackBerry

UEM, lorsque vous tentez d'enregistrer vos informations de locataire, le message d'erreur « La demande de connexion UEM n'est pas valide » s'affiche et vous ne pouvez pas enregistrer les informations. Pour obtenir des instructions sur l'activation du connecteur BlackBerry UEM, rendez-vous sur support.blackberry.com/community pour lire l'article 97480. Par défaut, ce connecteur est activé dans les environnements BlackBerry UEM Cloud.
  - Les comptes des utilisateurs doivent utiliser les mêmes comptes Active Directory ou Entra ID sur la console Cylance.
  - Cylance Endpoint Security prend en charge une connexion à un domaine UEM.
  - Vous devez Utiliser BlackBerry UEM pour installer l'application CylancePROTECT Mobile sur des terminaux. L'application doit être distribuée à partir d'UEM car elle nécessite des configurations d'application qui ne sont pas présentes si les utilisateurs téléchargent et installent l'application à partir de l'App Store ou de Google Play.
  - Pour connaitre les conditions préalables des terminaux iOS, consultez la section Conditions préalables : Vérifier que les terminaux iOS sont gérés par UEM.
  - Pour connaitre les conditions préalables des terminaux Android, consultez la section Conditions préalables : Vérifier que les terminaux Android sont gérés par UEM
- Microsoft Intune
  - Le compte d'administrateur Cylance Endpoint Security que vous utilisez pour vous connecter à Intune doit disposer d'une licence Intune.
  - Cylance Endpoint Security prend en charge une connexion à une instance Intune.
  - Tous les terminaux gérés par Intune doivent être inclus dans une stratégie de configuration d'applications dans la console Cylance. Pour plus d'informations, reportez-vous à Connecter Cylance Endpoint Security à Intune.

#### Conditions préalables : Vérifier que les terminaux iOS sont gérés par UEM

Il est nécessaire d'activer les terminaux iOS à l'aide de l'un des types d'activation suivants* :

- Contrôles MDM
- Confidentialité de l'utilisateur
- Confidentialité de l'utilisateur - Inscription de l'utilisateur

Si vos utilisateurs sont activés avec le type d'activation Confidentialité de l'utilisateur, effectuez l'une des tâches suivantes :

| Tâche | Étapes |
|---|---|
| Utiliser Cylance Endpoint Security pour gérer le VPN par application | 1. Dans le type d'activation Confidentialité de l'utilisateur, décochez la case **Autoriser la gestion des VPN** et cochez la case **Autoriser la gestion des applications**.<br>2. Dans la console Cylance Endpoint Security, configurez les options du service Gateway. |
| Utiliser UEM pour gérer le VPN par application | 1. Dans le profil d'activation Confidentialité de l'utilisateur, cochez les cases **Autoriser la gestion des VPN** et **Autoriser la gestion des applications**.<br>2. Créez un profil VPN personnalisé. Dans le champ **ID d'offre VPN**, saisissez l'ID de l'offre CylancePROTECT Mobile, `com.blackberry.protect`.<br>3. Dans la console Cylance Endpoint Security, configurez les options du service Gateway. |

* Si vous souhaitez désactiver un terminal de l'instance UEM, utilisez la commande Supprimer les données professionnelles uniquement pour supprimer les données professionnelles (par exemple, la stratégie IT, les

profils, les applications et les certificats) qui se trouvent sur le terminal. Si vous sélectionnez la commande Supprimer le terminal, le terminal est supprimé de votre instance UEM, mais les données et les profils ne sont pas supprimés et le terminal peut continuer à recevoir des e-mails et d'autres données professionnelles. BlackBerry vous recommande d'utiliser la commande Supprimer le terminal uniquement si un terminal est définitivement perdu ou endommagé et ne contactera donc plus le serveur. Pour en savoir plus sur les commandes que vous pouvez envoyer aux terminaux, consultez la section Commandes pour les terminaux iOS dans le contenu BlackBerry UEM.

**Conditions préalables : Vérifier que les terminaux Android sont gérés par UEM**

Il est possible d'activer les terminaux Android à l'aide de l'un des types d'activation suivants :

- Travail et personnel - Confidentialité de l'utilisateur (Android Enterprise avec profil professionnel)
- Espace Travail uniquement (terminal Android Enterprise entièrement géré)
- Travail et Personnel - Contrôle total (terminal Android Enterprise entièrement géré avec un profil professionnel)
- Espace Travail uniquement (Samsung Knox)
- Travail et Personnel - Contrôle total (Samsung Knox)
- Travail et Personnel - Confidentialité de l'utilisateur (Samsung Knox)

## Ajouter un connecteur BlackBerry UEM

Par défaut, la page Connecteurs affiche le nom, le type de connexion et l'état de la connexion du connecteur BlackBerry UEM en cours d'utilisation dans votre environnement. Votre locataire Cylance Endpoint Security prend en charge une connexion à un domaine UEM.

**Avant de commencer :** Vérifiez les conditions préalables pour le connecteur BlackBerry UEM.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Connecteurs**.
2. Cliquez sur **Ajouter un connecteur**, puis sélectionnez **BlackBerry UEM** dans la liste déroulante.
3. Sur l'écran **Informations sur le locataire**, saisissez l'ID SRP et la clé d'authentification du locataire BlackBerry UEM.
4. Cliquez sur **Enregistrer**.

## Utiliser BlackBerry UEM pour installer l'application CylancePROTECT Mobile sur des terminaux

Vous pouvez utiliser UEM pour installer l'application CylancePROTECT Mobile sur les terminaux. L'application doit être distribuée à partir d'UEM, car elle nécessite des configurations d'application qui ne sont pas présentes si les utilisateurs téléchargent et installent l'application à partir du site Web BlackBerry, de l'App Store ou de Google Play.

**Remarque :**

Tenez compte des limitations de fonctionnalités suivantes lorsque vous utilisez UEM pour installer l'application CylancePROTECT Mobile sur les terminaux :

- Pour les terminaux avec les types d'activation Confidentialité de l'utilisateur ou Contrôle total d'Android Enterprise, l'analyse des messages SMS n'est pas prise en charge.
- Pour les terminaux avec n'importe quel type d'activation Android Enterprise, la détection du verrouillage de l'écran n'est pas prise en charge.

**Avant de commencer :** Examinez Conditions préalables : Vérifier que les terminaux sont gérés par MDM.

1. Suivez les instructions du contenus relatifs à l'administration d'UEM pour ajouter l'application CylancePROTECT Mobile à la liste des applications :
   - Ajouter une application iOS à la liste des applications
   - Ajouter une application Android à la liste des applications

Spécifiez les paramètres de configuration d'application suivants :

| OS | Paramètres de configuration d'application |
|---|---|
| iOS | • Nom de la configuration de l'application : *name*<br>• Clé : uemperimeterid<br>• Valeur : %perimeterid% |
| Android | Nom : *name*<br>Les paramètres suivants sont préremplis :<br>• ID utilisateur : userid<br>• ID de périmètre UEM : %perimeterid% |

2. Attribuez l'application CylancePROTECT Mobile à des utilisateurs ou des groupes.
3. Définissez la disposition de l'application CylancePROTECT Mobile sur Requis.

**À la fin :**

- Demandez aux utilisateurs d'activer l'application CylancePROTECT Mobile à l'aide des informations qu'ils ont reçues dans leur e-mail d'activation. Cylance Endpoint Security envoie l'e-mail d'activation après l'attribution d'une politique d'inscription.
- Suivez les instructions pour Connexion de Cylance Endpoint Security aux solutions MDM pour vérifier si les terminaux sont gérés.

## Connecter Cylance Endpoint Security à Intune

**Avant de commencer :**

Le compte administrateur Cylance Endpoint Security que vous utilisez pour vous connecter à Intune doit disposer d'une licence Intune.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Connecteurs**.
2. Cliquez sur **Ajouter le connecteur** et sélectionnez **Microsoft Intune** dans la liste déroulante.
3. Indiquez votre ID de locataire Entra. Cliquez sur **Suivant**.
4. Spécifiez vos informations d'identification d'administrateur pour Entra.
5. Sur l'écran **Stratégies de configuration d'application**, activez les plateformes de système d'exploitation auxquelles appliquer l'intégration Intune et effectuez les étapes suivantes pour chaque plateforme. Tous les terminaux gérés par Intune avec lesquels vous utilisez cette fonctionnalité doivent être inclus dans une stratégie de configuration d'application. Pour créer des stratégies de configuration d'application ultérieurement, cliquez sur **Annuler**.
   a) Vous pouvez également modifier le nom de la stratégie. Ne modifiez pas l'application cible.
   b) Si vous souhaitez que la stratégie s'applique à tous les groupes de l'instance Intune, activez **Tous les groupes**.
   c) Si vous souhaitez que la stratégie s'applique à des groupes spécifiques de l'instance Intune, cliquez sur ⊕. Recherchez et sélectionnez des groupes, puis cliquez sur **Ajouter**.
6. Cliquez sur **Enregistrer**. Si vous avez ajouté une stratégie de configuration d'application pour Android, suivez les invites de consentement de l'administrateur qui s'affichent.

Les stratégies de configuration d'application que vous créez sont visibles dans le centre d'administration Intune.

**À la fin :**

- Demandez à l'administrateur Intune de votre organisation de modifier le connecteur CylancePROTECT Mobile MTD dans le centre d'administration Intune et d'activer les options suivantes. Pour activer le connecteur, procédez comme suit :
  1. Connectez-vous au centre d'administration Intune.
  2. Cliquez sur **Administration des locataires > Connecteurs et jetons**.
  3. Dans la section **Multiplateforme**, cliquez sur **Défense contre les menaces mobiles**.
  4. Cliquez sur **Ajouter**.
  5. Dans la liste déroulante **Sélectionner le connecteur Défense contre les menaces mobiles à configurer**, sélectionnez **CylancePROTECT Mobile**.
  6. Cliquez sur **Créer**.
- Pour ajouter des stratégies de configuration d'application ultérieurement ou si vous souhaitez ajouter des stratégies supplémentaires, dans **Paramètres > Connecteurs**, cliquez sur **Générer une configuration d'application** pour la connexion Intune.
- Si vous souhaitez également connecter Cylance Endpoint Security à Intune pour gérer les niveaux de risques des terminaux, consultez la section Intégration d'Cylance Endpoint Security à Microsoft Intune pour répondre aux menaces mobiles.

# Installation de l'agent CylanceGATEWAY

L'agent CylanceGATEWAY protège les terminaux Windows 10, Windows 11 et macOS des utilisateurs en vous permettant de bloquer les connexions aux destinations Internet auxquelles vous ne souhaitez pas accéder, même lorsque le terminal n'est pas connecté à votre réseau. BlackBerry tient constamment à jour une liste toujours plus longue de destinations Internet dangereuses afin d'empêcher les points de terminaison de s'y connecter. Si votre organisation souhaite également empêcher les utilisateurs de consulter des sites spécifiques qui ne répondent pas à vos normes d'utilisation acceptable, vous pouvez créer des stratégies pour spécifier des destinations supplémentaires auxquelles tous les utilisateurs ou certains utilisateurs ou groupes ne peuvent pas accéder.

L'agent CylanceGATEWAY est installé sur les terminaux des utilisateurs, afin que ces derniers puissent accéder aux ressources réseau en toute sécurité et protéger leurs terminaux contre les activités réseau suspectes et potentiellement malveillantes. Lorsque l'agent CylanceGATEWAY est installé et que le mode de travail est activé, CylanceGATEWAY établit des connexions sécurisées entre le terminal de l'utilisateur et le réseau de votre entreprise et l'Internet public, analyse l'activité de votre réseau et applique les stratégies d'accès réseau que vous avez définies. Lorsque vous activez le mode sans échec pour les terminaux macOS Windows, CylanceGATEWAY étend les règles ACL du locataire et la protection des points de terminaison des terminaux lorsque le mode de travail n'est pas activé afin que les terminaux soient toujours protégés si le trafic réseau n'emprunte pas le tunnel.

Lorsque vous déployez une nouvelle installation de l'agent CylanceGATEWAY, il convient de redémarrer les terminaux des utilisateurs, et de demander aux utilisateurs de terminer manuellement le processus d'installation et d' activer le mode de travail ou d'activer le mode sans échec. Lorsque vous déployez une mise à niveau de l'agent CylanceGATEWAY, les utilisateurs doivent redémarrer leurs terminaux pour que la mise à niveau prenne effet. Pendant la mise à niveau, l'agent CylanceGATEWAY conserve toutes les configurations. Aucune action supplémentaire n'est requise de la part des utilisateurs.

Lorsque l'installation de l'agent CylanceGATEWAY est contrôlée par des outils de gestion des terminaux d'entreprise (par exemple, System Center Configuration Manager (SCCM) de Microsoft ou tout autre outil de déploiement), vous pouvez inclure les paramètres customDomain pour minimiser l'interaction de l'utilisateur une fois l'agent activé. Vous pouvez obtenir le nom de domaine personnalisé à partir du champ Nom de domaine personnalisé sous Paramètres > Application. Vous pouvez fournir les paramètres pour les terminaux Windows à partir de la ligne de commande et pour les terminaux macOS à l'aide d'une configuration d'application gérée ou de préférences d'application MCX. Vous pouvez également demander aux utilisateurs de télécharger et d'installer manuellement l'agent CylanceGATEWAY pour activer le mode de travail ou activer le mode sans échec.

- Pour les terminaux macOS, incluez la valeur suivante pour spécifier le nom de domaine personnalisé à utiliser lorsque les utilisateurs activent l'agent CylanceGATEWAY 2.9 ou version ultérieure :

  ```
  <dict>
    <key>customDomain</key>
    <string>Your_custom_domain_name</string>
  </dict>
  ```

- Pour les terminaux Windows, incluez la commande suivante pour spécifier le nom de domaine personnalisé à utiliser lorsque les utilisateurs activent l'agent CylanceGATEWAY 2.9 ou version ultérieure :

  `CylanceGATEWAY-<version>.exe /v"CUSTOM_DOMAIN=<your_custom_domain_name>"`

  Pour spécifier le nom de domaine personnalisé pour une installation silencieuse, reportez-vous à la section Effectuer une installation et une mise à niveau en mode silencieux de l'agent CylanceGATEWAY.

## Effectuer une installation et une mise à niveau en mode silencieux de l'agent CylanceGATEWAY

Vous pouvez déployer l'agent CylanceGATEWAY pour les utilisateurs. Si le déploiement concerne une nouvelle installation, les utilisateurs doivent redémarrer leur terminal et terminer manuellement le processus d'installation, puis activer le mode de travail ou activer le mode sans échec. Pour les nouveaux déploiements, vous pouvez spécifier le nom de domaine personnalisé que vous obtenez dans le champ Nom de domaine personnalisé sous Paramètres > Application. Si le déploiement est une mise à niveau, les utilisateurs doivent redémarrer leurs terminaux pour appliquer la mise à niveau. Les configurations de l'agent CylanceGATEWAY sont conservées et aucune action supplémentaire n'est requise de la part des utilisateurs.

**Avant de commencer :** Téléchargez une copie de l'agent CylanceGATEWAY pour Windows depuis le site Web BlackBerry et enregistrez-la dans un emplacement sur votre ordinateur.

1. Ouvrez l'invite de commande en tant qu'administrateur.
2. Accédez à l'emplacement où vous avez enregistré les agents CylanceGATEWAY. Effectuez l'une des tâches suivantes. Dans cet exemple, nous utiliserons la version 2.7.0.19 de l'agent CylanceGATEWAY.
   - Pour effectuer une installation ou une mise à niveau en mode silencieux sans redémarrer les terminaux des utilisateurs, saisissez

     `.\CylanceGATEWAY-2.7.0.19.exe /s /v" REBOOT=Suppress /qn"`
   - Pour effectuer une installation ou une mise à niveau en mode silencieux et redémarrer immédiatement les terminaux des utilisateurs, saisissez `.\CylanceGATEWAY-2.7.0.19.exe /s /v" /qn"`
   - Pour effectuer une installation ou une mise à niveau en mode silencieux et créer un fichier journal d'installation appelé GWInstall, saisissez

     `.\CylanceGATEWAY-2.7.0.19.exe /s /v" REBOOT=Suppress /qn /l*v .\GWInstall.log"`
   - Pour effectuer une nouvelle installation et spécifier le nom de domaine personnalisé, saisissez

     `.\CylanceGATEWAY-<2.9.x.x>.exe /s /v" CUSTOM_DOMAIN=<your_custom_domain_name> /qn"`

     Pour utiliser cette fonctionnalité, vous devez disposer de l'agent CylanceGATEWAY pour Windows 2.9 ou version ultérieure.
3. Si nécessaire, demandez à vos utilisateurs de redémarrer leurs terminaux et de suivre les instructions à l'écran.

# Configurer CylanceAVERT

| Élément | Description |
|---|---|
| 1 | Consulter la configuration logicielle requise |
| 2 | Définir le contenu sensible |
| 3 | Installer CylanceAVERT |
| 4 | Créer des stratégies de protection des informations |
| 5 | Attribuer des stratégies à des administrateurs, des utilisateurs et des groupes |

## Installation de l'agent CylanceAVERT

Vous pouvez télécharger et installer CylanceAVERT à partir de la page Téléchargements du portail BlackBerry myAccount.

Vous pouvez installer CylanceAVERT en mode silencieux via SCCM ou JAMF pour l'utilisateur. Pour ce faire, vous devrez inclure le paramètre de ligne de commande `IAgreetoBBSLA=true` pour accepter le contrat de licence de l'utilisateur final (EULA). L'EULA ne sera pas affiché pour l'utilisateur. Après l'installation en mode silencieux CylanceAVERT, vous devez redémarrer le système.

**Remarque :** Avant de procéder à l'installation en mode silencieux de CylanceAVERT, vous devez lire le Contrat de licence de la solution BlackBerry, y compris la Déclaration de confidentialité BlackBerry. Vous ne pouvez installer l'application que si vous acceptez les conditions générales du contrat de licence de la solution BlackBerry de la manière indiquée ci-dessus. **Si vous n'acceptez pas les conditions générales du contrat de licence de la solution BlackBerry, n'installez pas et n'utilisez pas CylanceAVERT**.

Une fois l'agent CylanceAVERT installé, l'utilisateur peut recevoir des notifications de sécurité pour le partage non autorisé potentiel de données sensibles de l'entreprise lors de l'envoi d'e-mails, du transfert de fichiers via USB et du chargement de fichiers sur un site Web.

Si un utilisateur qui n'est pas ajouté à Cylance Endpoint Security se connecte à un poste de travail CylanceAVERT qui a été installé, il est automatiquement ajouté à Cylance Endpoint Security avec toutes les stratégies qui lui sont appliquées. Cela nécessite Active Directory ou une connexion au répertoire BlackBerry Connectivity Node. Si vous utilisez une connexion au répertoire BlackBerry Connectivity Node pour la gestion des utilisateurs, vous devez utiliser BlackBerry Connectivity Node version 2.12.1 ou ultérieure. Pour plus d'informations, reportez-vous aux sections Installation de BlackBerry Connectivity Node et Association à votre annuaire d'entreprise dans le Guide de configuration de Cylance Endpoint Security.

**Remarque :** Si un utilisateur quitte l'application CylanceAVERT depuis le panneau des applications Windows, il ne recevra pas de notification Windows lorsqu'un évènement d'exfiltration se produit.

### Installer CylanceAVERT

CylanceAVERT nécessite CylancePROTECT Desktop version 3.1 ou versions ultérieures.

**Remarque :** CylanceAVERT ne peut pas être installé sur un ordinateur avec CylancePERSONA.

1. Sur le terminal, double-cliquez sur le programme d'installation CylanceAVERT de l'agent.
2. Suivez les étapes d'installation.

**À la fin :**

- Pour vérifier que l'agent CylanceAVERT est installé, vérifiez les points suivants :
  - L'icîne CylanceAVERT apparait dans la barre d'état système
  - L'utilisateur CylanceAVERT apparait dans la liste des utilisateurs de la page Actifs de la console.
  - Dans le Gestionnaire des tâches Windows, vérifiez que le processus CylanceAVERT est en cours d'exécution.
- Pour désinstaller l'agent, utilisez les paramètres Windows.

**Remarque :** Une fois CylanceAVERT installé, le plug-in du navigateur empêche le chargement de fichiers sur des sites Web non sécurisés (non SSL). BlackBerry vous recommande de ne pas tenter de charger des fichiers sur des sites Web non SSL.

## Définir le contenu sensible à l'aide des paramètres de protection des informations

Avec les paramètres de protection des informations, vous pouvez spécifier les types de données que CylanceAVERT recherchera dans les fichiers sensibles, les preuves collectées, les domaines d'e-mail et de navigateur que vous souhaitez considérer comme fiables et les adresses e-mail auxquelles vous souhaitez envoyer les notifications d'un évènement d'exfiltration.

### Gérer la collecte de preuves

Vous pouvez personnaliser la manière dont les évènements d'exfiltration de données sont collectés dans CylanceAVERT. Les paramètres de collecte de données vous permettent de configurer les preuves que vous souhaitez collecter lors d'un évènement d'exfiltration de données à des fins d'audit. En configurant les paramètres de collecte de données, vous pouvez prendre des décisions telles que l'inclusion d'extraits de fichiers de l'évènement d'exfiltration, l'enregistrement de copies complètes des fichiers impliqués dans l'évènement d'exfiltration, la gestion des chargements dans le casier de preuves, la sélection des heures de téléchargement des fichiers, et spécifier la durée pendant laquelle les preuves de données doivent être conservées.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Protection des informations**.
2. Cliquez sur l'onglet **Collecte de données**.
3. Effectuez l'une des opérations suivantes pour configurer les paramètres de protection des informations :

| Élément | Étapes |
| --- | --- |
| Extraits de fichier | Cliquez sur le bouton **Générer des extraits de fichier** pour activer ou désactiver la collecte de fragments de fichier. Lorsque l'option **Générer des extraits de fichier** est activée, un extrait de fichier de l'évènement d'exfiltration de données est enregistré dans les détails des évènements. Par défaut, l'option **Générer des extraits de fichier** est désactivée. |

| Élément | Étapes |
| --- | --- |
| Collecte des fichiers de preuve | • Cliquez sur le bouton **Activer la collecte de fichiers de preuve** pour activer ou désactiver la collecte de fichiers de preuve. Par défaut, l'option **Activer la collecte de fichiers de preuve** est désactivée. Lorsque l'option **Activer la collecte de fichiers de preuve** est activée, une copie complète des fichiers impliqués dans un évènement d'exfiltration de données est enregistrée dans les détails de l'évènement. Pour plus d'informations, consultez la section Afficher les informations sur l'évènement CylanceAVERT.<br>• Cliquez sur le champ de texte **Espace disque** et saisissez une valeur pour spécifier la quantité maximale d'espace disque disponible que vous pouvez allouer à la mise en cache des fichiers de preuve sur des terminaux distants ou un casier de preuves. Par défaut, **Espace disque** est défini sur 10 %. |
| Charger un fichier | Cliquez sur le menu déroulant **Méthode de chargement de fichiers** et sélectionnez une méthode. En sélectionnant **Direct**, les terminaux de votre réseau pourront télécharger des fichiers directement dans votre casier de preuves. Si l'accès direct à votre casier de preuves est bloqué (par exemple, par votre pare-feu), BlackBerry téléchargera les fichiers via son nuage en sélectionnant **Service BlackBerry Proxy**. Par défaut, **Direct** est sélectionné. |
| Conserver les fichiers de preuve | Cliquez sur le menu déroulant **Conservation des données** et sélectionnez la durée pendant laquelle vous souhaitez que les fichiers de preuve soient stockés dans votre casier de preuves. La durée de stockage des fichiers de preuve est de 30, 60 ou 90 jours. Par défaut, **Conservation des données** est définie sur 30 jours. |

## Ajouter des domaines autorisés et de confiance

Vous spécifiez des domaines afin de pouvoir répertorier les adresses de navigateur et d'e-mail auxquelles vous pouvez faire confiance pour télécharger des fichiers en toute sécurité. Après avoir ajouté des domaines, vous devez les activer pour les utiliser dans les stratégies de protection des informations. Lorsque vous spécifiez un domaine autorisé pour une stratégie, il ne déclenche aucune violation de stratégie lors de l'analyse des chargements de fichiers sensibles si le domaine a été validé par rapport à un certificat ajouté et qu'il devient un domaine de confiance. Si vous ne spécifiez aucun domaine dans les paramètres de protection des informations ou si vous n'ajoutez aucun domaine à utiliser dans vos stratégies, tous les domaines seront traités comme non approuvés.

**Remarque :**

- Tous les domaines de terminaux USB sont considérés comme non approuvés.
- Une fois que vous avez spécifié un domaine autorisé, tous les sous-domaines sont également considérés comme autorisés tant que leurs certificats de confiance sont ajoutés.

**Avant de commencer :** Vérifiez qu'un certificat de confiance est chargé. Pour qu'un domaine soit considéré comme fiable, un certificat approuvé doit être téléchargé. Si un certificat de confiance n'est pas téléchargé et que le domaine autorisé est utilisé dans une stratégie, il déclenche toujours un évènement d'exfiltration. Pour plus d'informations, reportez-vous à Vérifier des domaines à l'aide de certificats de confiance.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Protection des informations**.
2. Cliquez sur l'onglet **Domaines autorisés**.
3. Pour ajouter un nouveau domaine de navigateur, cliquez sur le bouton **Ajouter un nouveau domaine**.

4. Dans la boite de dialogue **Ajouter un domaine autorisé**, saisissez un nom et une description pour le domaine dans les champs de texte. Les caractères génériques ne sont pas pris en charge dans le champ de nom de domaine.
5. Vous pouvez également activer la possibilité d'utiliser ce domaine dans une stratégie.
6. Cliquez sur **Vérifier** pour vérifier si ce domaine utilise un certificat approuvé existant. Si aucun certificat n'est chargé, ajoutez-en un maintenant. Pour obtenir des instructions, reportez-vous à Vérifier des domaines à l'aide de certificats de confiance.
7. Cliquez sur **Ajouter**.
8. Si vous souhaitez ajouter un nouveau domaine de messagerie, saisissez-le dans la section **Domaines de messagerie autorisés** et utilisez une virgule pour le séparer des domaines précédemment saisis.

**À la fin :**

Pour supprimer un domaine autorisé, dans la liste **Domaines autorisés**, cochez la case près du domaine de votre choix, puis cliquez sur **Supprimer**.

## Utiliser des modèles pour regrouper les types de données

Vous pouvez utiliser des modèles pour regrouper les types de données sensibles que votre entreprise doit utiliser dans une stratégie.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Protection des informations**.
2. Cliquez sur l'onglet **Modèles**.
3. Pour ajouter un modèle prédéfini, cliquez sur **Ajouter prédéfini**, sélectionnez les modèles prédéfinis dans la liste et cliquez sur **Ajouter**.
4. Pour créer un modèle personnalisé, cliquez sur **Créer un modèle personnalisé**.
5. Sur la page **Ajouter un nouveau modèle**, dans la section **Informations générales**, saisissez le nom du modèle et sélectionnez la région dans la liste déroulante.
6. Dans le menu déroulant **Région**, sélectionnez la région pour laquelle le modèle sera utilisé. Par exemple, si vous créez un modèle avec les types de données Carte d'assurance maladie canadienne et Numéro SIN canadien, sélectionnez Canada comme région.
7. Dans le menu déroulant **Type d'informations**, sélectionnez le type d'informations correspondant à votre modèle. Les valeurs sont des données personnalisées, financières, de santé et personnelles.
8. Dans la section **Générateur de conditions**, sélectionnez le type de données dans la liste déroulante et spécifiez le nombre minimal d'occurrences requises pour déclencher la violation de règle. Pour ajouter un autre type de données au groupe, cliquez sur **Ajouter un élément**.
   - Pour ajouter un autre type de données au groupe, cliquez sur **Ajouter un élément**.
   - Pour ajouter un autre groupe de conditions, cliquez sur **Ajouter un groupe**.
9. Cliquez sur **Enregistrer**.

**À la fin :**

Une fois votre modèle ajouté, vous pouvez l'ajouter à une stratégie de protection des informations. Pour plus d'informations, reportez-vous à Gérer des stratégies de protection des informations.

Pour supprimer un modèle, dans la colonne **Actions** en regard du modèle que vous souhaitez supprimer, procédez comme suit :

- Pour supprimer un modèle prédéfini, cliquez sur ⊗. Dans la boite de dialogue de confirmation, cliquez sur **Supprimer**.
- Pour supprimer un modèle personnalisé, cliquez sur 🗑. Dans la boite de dialogue de confirmation, cliquez sur **Supprimer**.

Lorsqu'un modèle est supprimé de votre liste, il ne sera plus disponible dans une stratégie de protection des informations.

Pour modifier un modèle personnalisé, cliquez sur le modèle dans la liste et modifiez les informations dans les champs. Vous ne pouvez pas modifier un modèle prédéfini. Reportez-vous aux étapes 4 à 7 pour plus d'informations.

Pour copier un modèle, cliquez sur  dans la colonne Actions du modèle que vous souhaitez copier.

## Spécifier des types de données sensibles

Les types de données représentent les données sensibles qu'CylanceAVERT analysera. Vous pouvez définir des types de données dans les paramètres de protection des informations et les personnaliser en fonction des besoins de votre entreprise. Les méthodes de recherche disponibles pour les types de données sont les mots-clés ou les expressions régulières.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Protection des informations**.
2. Cliquez sur l'onglet **Types de données**.
3. Cliquez sur **Ajouter un type de données personnalisé**.

   **Remarque :** Vous pouvez également ajouter des types de données prédéfinis à votre liste, ce qui permet d'utiliser le type de données dans une stratégie de protection des informations. Pour ajouter un type de données prédéfini à une liste, cliquez sur **Ajouter un type de données prédéfini**, sélectionnez les types de données prédéfinis que vous souhaitez ajouter à votre liste, puis cliquez sur **Ajouter**.
4. Sur la page **Ajouter un type de données personnalisé**, ajoutez un nom et une description pour le nouveau type de données.
5. Dans la liste déroulante **Région**, sélectionnez la région pour laquelle le type de données sera utilisé. Par exemple, si vous souhaitez rechercher un numéro de permis de conduire canadien, sélectionnez Canada comme région.
6. Dans le menu déroulant **Type d'informations**, sélectionnez le type d'informations correspondant à votre type de données. Les valeurs sont des données personnalisées, financières, de santé et personnelles.
7. Dans le menu déroulant **Méthode de recherche**, sélectionnez la méthode de recherche que vous souhaitez utiliser. Les valeurs sont des mots-clés, des expressions ou un dictionnaire de mots-clés. Un dictionnaire de mots-clés est un fichier texte qui spécifie plusieurs mots-clés. Pour créer un dictionnaire de mots-clés, vous devez créer un fichier texte avec chaque mot-clé écrit sur une nouvelle ligne.
8. Effectuez l'une des opérations suivantes :

   - Si vous avez sélectionné **Mots-clés** comme méthode de recherche, saisissez les mots-clés que vous souhaitez rechercher dans le champ **Mots-clés**. Vous pouvez utiliser des virgules pour séparer plusieurs mots-clés.
     - Sélectionnez **Correspondance exacte** pour considérer le fichier comme sensible si les mots-clés correspondent exactement. Lorsque cette option est sélectionnée, les mots-clés ne sont pas mis en correspondance s'ils font partie d'une chaine de texte plus grande. Par exemple, si vous spécifiez le mot-clé « confidentiel », « confidentialité » ne renvoie aucune correspondance.
     - Sélectionnez **Appliquer la sensibilité à la casse** pour considérer le fichier comme sensible si la casse des mots-clés correspond exactement. Si cette option est sélectionnée, la casse du texte est appliquée. Par exemple, si vous spécifiez le mot-clé « confidentiel », « CONFIDENTIEL » ne renvoie aucune correspondance.
   - Si vous avez sélectionné **Expression régulière (RegEx)** comme méthode de recherche, saisissez l'expression régulière que vous souhaitez rechercher dans le champ **Regex**.

     **Remarque :** Si vous utilisez la regex, notez ce qui suit :

     - La méthode regex doit être conforme au langage d'expression .NET.

    - Vous pouvez valider la regex à l'aide d'outils populaires tels que Regex101 ou Regex Storm.
- Si vous avez sélectionné **Dictionnaire des mots-clés**, procédez comme suit :
    - Sélectionnez **Correspondance exacte** pour considérer le fichier comme sensible si les mots-clés correspondent exactement. Lorsque cette option est sélectionnée, les mots-clés ne sont pas mis en correspondance s'ils font partie d'une chaine de texte plus grande. Par exemple, si vous spécifiez le mot-clé « confidentiel » dans votre dictionnaire de mots-clés, « confidentialité » ne renvoie aucune correspondance.
    - Sélectionnez **Appliquer la sensibilité à la casse** pour considérer le fichier comme sensible si la casse des mots-clés correspond exactement. Si cette option est sélectionnée, la casse du texte est appliquée. Par exemple, si vous spécifiez le mot-clé « confidentiel » dans votre dictionnaire de mots-clés, « CONFIDENTIEL » ne renvoie aucune correspondance.
    - Cliquez sur **Charger le dictionnaire de mots-clés** et sélectionnez votre dictionnaire de mots-clés. Vous ne pouvez charger qu'un seul fichier de dictionnaire de mots-clés par type de données.

    **Remarque :** Les restrictions suivantes s'appliquent à un dictionnaire de mots-clés :

    - La taille combinée de tous les dictionnaires de mots-clés d'un locataire ne peut pas dépasser 1,5 Mo.
    - Un mot-clé unique dans le dictionnaire de mots-clés ne peut pas comporter plus de 1 024 caractères.
    - Le nombre maximal d'entités de données de dictionnaire de mots-clés sur un locataire est de 1 000.
9. Cliquez sur **Créer**.

**À la fin :**

- Le type de données personnalisé peut être supprimé. Pour supprimer un type de données personnalisé, cliquez sur dans la colonne **Actions**. Dans la fenêtre contextuelle de confirmation, cliquez sur **Supprimer**. **Remarque :** Vous recevrez une fenêtre contextuelle **Type de données utilisé** si le type de données est utilisé dans une stratégie et vous ne pourrez pas le supprimer tant qu'il n'aura pas été supprimé.
- Un type de données prédéfini peut être retiré de votre liste, mais pas supprimé. Pour supprimer un type de données prédéfini de votre liste, cliquez sur dans la colonne **Actions**. Dans la fenêtre contextuelle de confirmation, cliquez sur **Supprimer**. Vous pouvez ajouter à nouveau un type de données prédéfini à votre liste en cliquant sur **Ajouter un type de données prédéfini** et en sélectionnant le type de données dans la liste. **Remarque :** Vous recevrez une fenêtre contextuelle **Type de données utilisé** si le type de données est utilisé dans une stratégie et vous ne pourrez pas le supprimer tant qu'il n'aura pas été supprimé.
- Il est possible de télécharger un fichier de dictionnaire de mots-clés existant. En cas de chargement d'un dictionnaire de mots-clés mis à jour, le point de terminaison est à nouveau analysé et les stratégies sont évaluées. Actuellement, les évènements existants restent évalués à partir du type de données précédent.

## Vérifier des domaines à l'aide de certificats de confiance

Les certificats approuvés vous permettent de vérifier les domaines de navigateur autorisés qui ont été ajoutés dans les paramètres de protection des informations. Si un certificat de confiance est manquant et que le domaine autorisé est utilisé dans une stratégie, il déclenche un évènement d'exfiltration. Pour en savoir plus sur les domaines autorisés, reportez-vous à Ajouter des domaines autorisés et de confiance.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Protection des informations**.
2. Cliquez sur l'onglet **Certificats de confiance**.
3. Cliquez sur **Ajouter le certificat**.
4. Chargez un fichier de certificat racine ou intermédiaire (.pem). Cliquez sur **Parcourir les fichiers** pour rechercher un fichier .pem local sur votre terminal, puis cliquez sur **Ajouter**.

### Envoyer des notifications à des adresses e-mail spécifiées

Vous pouvez spécifier les adresses e-mail auxquelles envoyer des notifications lorsqu'un évènement d'exfiltration de données se produit ou lorsque le casier de preuves atteint sa capacité de stockage. Seuls les administrateurs Cylance Endpoint Security peuvent voir les détails des évènements, mais n'importe quel utilisateur peut recevoir des notifications.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Protection des informations**.
2. Cliquez sur l'onglet **Notifications**.
3. Activez l'option **Activer les notifications d'évènements de protection des informations** pour activer l'envoi de notifications par e-mail pour les évènements CylanceAVERT à des destinataires d'e-mail spécifiés.
4. Dans le champ de texte **Destinataires des e-mails**, saisissez les adresses e-mail pour lesquelles vous souhaitez recevoir des notifications d'évènements CylanceAVERT. Vous pouvez utiliser une virgule pour séparer plusieurs adresses e-mail.
5. Activez l'option **Activer les notifications de stockage du casier de preuves** pour activer l'envoi de notifications par e-mail pour la capacité de stockage du casier de preuves à des destinataires d'e-mails spécifiés.
6. Dans le champ de texte **Destinataires des e-mails**, saisissez les adresses e-mail auxquelles vous souhaitez recevoir les notifications de capacité de stockage du casier de preuves. Vous pouvez utiliser une virgule pour séparer plusieurs adresses e-mail.

## Gérer des stratégies de protection des informations

Les stratégies de protection des informations vous permettent de créer des stratégies organisationnelles ou règlementaires déclenchées lorsque des conditions spécifiques sont remplies. Vous pouvez ajouter des conditions à l'aide d'un modèle ou via le générateur de conditions. Les stratégies de protection des informations sont cumulatives et ne sont pas classées comme d'autres stratégies Cylance Endpoint Security. Si l'utilisateur est inconnu ou si aucune stratégie n'a été attribuée, toutes les stratégies seront appliquées à l'utilisateur.

Les stratégies de protection des informations peuvent être règlementaires ou organisationnelles. Selon le type de stratégie, une logique de rapprochement différente sera appliquée.

- Lorsqu'un utilisateur se voit attribuer plusieurs types de stratégies règlementaires, les stratégies sont consolidées pour l'utilisateur et les règles et actions de correction les plus restrictives sont appliquées.
- Lorsqu'un utilisateur se voit attribuer plusieurs types de stratégies organisationnelles, les stratégies sont consolidées pour l'utilisateur et les règles et actions de correction les moins restrictives sont appliquées.

**Remarque :** Au moins une règle de protection des informations est requise. Si vous essayez de supprimer les stratégies de protection des informations, vous recevrez un message d'erreur indiquant qu'une stratégie est requise.

### Appliquer les bonnes pratiques de consolidation des règles

CylanceAVERT dispose de deux types de conformité aux stratégies qui peuvent être utilisés dans une stratégie de protection des informations.

La conformité règlementaire fait référence à un ensemble limité de données sensibles utilisées pour protéger les informations sensibles liées aux règlementations sectorielles ou gouvernementales. Les données règlementaires sont des données qui ne changent pas au fil du temps. Les types de données prédéfinis dans les paramètres CylanceAVERT sont tous règlementaires et vous sont fournis par BlackBerry pour accélérer et simplifier la configuration du produit. Vous pouvez créer vos propres types de données règlementaires et modèles à utiliser dans une stratégie qui encapsule toutes les données règlementaires dont votre entreprise a besoin. Par exemple, au lieu d'utiliser le modèle fourni par BlackBerry, vous pouvez créer une politique règlementaire de Santé du Canada qui combine un numéro SIN canadien, un numéro PHIN, un numéro de service de santé, un permis de conduire, un numéro de compte bancaire, et le numéro de passeport dans une seule police. CylanceAVERT

utilise une expression régulière ou une correspondance de mots-clés pour déterminer si un fichier contient des informations règlementaires pertinentes, comme indiqué dans la politique.

La conformité organisationnelle fait référence à un ensemble infini de données où le contenu et les personnes qui peuvent accéder aux données changent constamment d'une organisation à l'autre en fonction de la situation organisationnelle. Par conséquent, la conformité organisationnelle doit être utilisée pour protéger les données sensibles qui contiennent des informations sur la propriété intellectuelle de l'entreprise ou d'autres informations pertinentes pour votre entreprise.

Il est possible que plusieurs stratégies s'appliquent au même fichier sensible, où elles entrent en conflit dans leur action de correction qu'elles prendront lorsqu'un fichier sensible est découvert. Dans ce cas, CylanceAVERT appliquera le rapprochement des mesures correctives pour ces stratégies.

Lorsque des collisions de stratégies se produisent, CylanceAVERT applique automatiquement le rapprochement. L'action de rapprochement diffère si le fichier enfreint une politique règlementaire, une politique organisationnelle ou les deux. Si un fichier est classé comme étant uniquement organisationnel, la mesure de correction la moins restrictive s'applique. Si un fichier est classé comme règlementaire et/ou organisationnel, la mesure la plus restrictive s'applique. Par exemple, si un fichier est soumis à une politique organisationnelle qui détermine qu'il est sensible s'il contient 2 occurrences du mot « confidentiel », et une seconde stratégie organisationnelle qui détermine la sensibilité en fonction de 3 occurrences du même mot, le fichier sera déterminé comme sensible pour 3 occurrences (le moins restrictif). Toutefois, si l'une de ces règles ou les deux étaient règlementaires, le fichier serait sensible avec 2 occurrences (plus restrictif).

## Créer un profil de protection des informations

1. Dans la barre de menus de la console de gestion, cliquez sur **Stratégies > Stratégie utilisateur**.
2. Cliquez sur l'onglet **Protection des informations**.
3. Cliquez sur l'onglet **Ajouter une stratégie**.
4. Dans la section **Informations générales**, remplissez les champs suivants :
   - Dans le champ **Nom de la stratégie**, saisissez un nom pour votre stratégie.
   - Dans le champ **Description**, saisissez une description pour votre stratégie.
   - Dans le menu déroulant **Type de stratégie**, sélectionnez le type de stratégie que vous créez. Les valeurs possibles pour le type de stratégie sont règlementaire ou organisationnel.
     - Un type de stratégie règlementaire fait référence à l'ensemble fini de données sensibles défini par une règlementation qui ne change pas nécessairement au fil du temps (par exemple, PCI, HIPAA, etc.).
     - Un type de stratégie organisationnelle fait référence aux données propriétaires de l'entreprise, où le public qui peut accéder aux données peut changer en permanence. Par conséquent, les données organisationnelles doivent être classées en éléments de données (par exemple, le type de fichier, les mots-clés, le créateur de fichier, le rôle du créateur de fichier, etc.).
5. Dans la section **Conditions**, configurez les conditions qui déclencheront une violation de stratégie en utilisant l'une des méthodes suivantes :

| Condition | Description |
|---|---|
| Ajouter des conditions à l'aide d'un modèle | **a.** Cliquez sur **Ajouter à partir du modèle**.<br>**b.** Cochez la case correspondant aux modèles que vous souhaitez ajouter à votre stratégie.<br>**Remarque :** Vous pouvez filtrer la liste des modèles à l'aide de la barre de recherche. |

| Condition | Description |
| --- | --- |
| Ajoutez des conditions à l'aide du générateur de conditions | **Remarque :** Le générateur de conditions est composé de groupes d'instructions **and** et **or**. Vous devez utiliser une combinaison de ces groupes d'instructions pour déterminer quand une stratégie sera déclenchée.<br>**a.** Dans la section des conditions **and**, sélectionnez les conditions dans la liste déroulante, puis spécifiez le nombre minimal d'occurrences requises pour déclencher la condition dans le menu déroulant numérique.<br>• Si vous souhaitez ajouter un autre élément à votre groupe d'instructions actuel, cliquez sur **Ajouter un élément**.<br>• Si vous souhaitez ajouter un autre groupe d'instructions, cliquez sur **Ajouter un groupe**.<br>• Si vous souhaitez supprimer un groupe d'instructions, cliquez sur **Supprimer le groupe**.<br>**b.** Dans la section des conditions **or**, sélectionnez les conditions dans la liste déroulante, puis spécifiez le nombre minimal d'occurrences requises pour déclencher la condition dans le menu déroulant numérique. |

6. Dans la section **Domaines autorisés**, cliquez sur ⊕, puis sélectionnez dans la liste le domaine de navigateur que vous souhaitez autoriser pour votre stratégie.
7. Dans la section **Domaines d'e-mails autorisés**, sélectionnez les destinataires d'e-mails spécifiés dans les paramètres de protection des informations qui doivent être autorisés pour votre stratégie.
8. Dans la section **Actions**, dans les listes déroulantes, sélectionnez l'action à effectuer pour les évènements de navigateur Web, USB et d'exfiltration d'e-mails. Sélectionnez l'une des actions suivantes :
   - Rapport : cette option signale l'exfiltration de données ou la violation de stratégie à la console Cylance Endpoint Security qui peut être affichée sur la page Événements Avert (Avert > Événements), crée une alerte dans la vue Alertes et envoie les événements à la solution SIEM ou au serveur syslog, le cas échéant. En outre, un e-mail est envoyé aux destinataires spécifiés dans l'écran Notifications (Paramètres > Protection des informations).
   - Rapport et notification : cette option signale l'exfiltration de données ou la violation de stratégie à la console Cylance Endpoint Security et affiche le badge d'exfiltration de données ou de violation de stratégie et la notification dans la barre des tâches du point de terminaison pour l'utilisateur.
   - Rapport, notification et avertissement : cette option signale l'exfiltration de données ou la violation de stratégie à la console Cylance Endpoint Security, affiche un badge et une notification dans la barre des tâches, et ajoute une notification Windows au point de terminaison et un avertissement contextuel à l'utilisateur avant que l'exfiltration de données ou la violation de stratégie ne se produise. Par exemple, si un utilisateur utilise Microsoft Outlook, l'agent CylanceAVERT intercepte l'e-mail et affiche une alerte dans l'éditeur d'e-mail ainsi qu'un avertissement à l'attention de l'utilisateur avant l'envoi des données sensibles.
9. Cliquez sur **Ajouter**.

   **Remarque :** Si un utilisateur a des stratégies qui lui sont attribuées, puis que toutes ces stratégies sont supprimées, l'utilisateur est supprimé de CylanceAVERT.

**À la fin :**

Effectuez l'une des opérations suivantes :

- Vous pouvez attribuer une stratégie aux utilisateurs et aux groupes d'utilisateurs. Pour plus d'informations, consultez la section Afficher les informations sur l'utilisateur CylanceAVERT.
- Pour supprimer une stratégie de protection des informations, cochez la case en regard de la stratégie dans la liste, puis cliquez sur **Supprimer**.

- Pour modifier une stratégie de protection des informations, cliquez sur la stratégie dans la liste, apportez une modification à la stratégie, puis cliquez sur **Enregistrer**.

# Gérer les mises à jour pour les agents CylancePROTECT Desktop et CylanceOPTICS

Vous pouvez utiliser des règles de mise à jour pour gérer les mises à jour des agents CylancePROTECT Desktop et CylanceOPTICS sur les terminaux. Les règles de mise à jour vous permettent de configurer Cylance Endpoint Security pour envoyer automatiquement les mises à jour vers une version spécifique ou la dernière version disponible, ou désactiver les mises à jour automatiques pour gérer la distribution logicielle à l'aide de la méthode choisie par votre organisation. Les zones sont associées à des règles de mise à jour, de sorte que les terminaux et les utilisateurs qui font partie de ces zones reçoivent les mises à jour en conséquence (également appelées mises à jour basées sur les zones). Par défaut, les règles de mise à jour Test, Pilote et Production sont disponibles, mais vous pouvez également ajouter des règles de mise à jour supplémentaires pour gérer les mises à jour des agents en fonction des besoins de votre organisation.

La version de l'agent sur le terminal est toujours mise à jour vers la version spécifiée dans la règle de mise à jour. Vous pouvez utiliser des règles de mise à jour pour installer une version antérieure d'un agent, même si le terminal utilise déjà une version plus récente.

Si le pilote Linux d'un terminal a été précédemment mis à jour manuellement sur un terminal, le pilote n'est pas automatiquement mis à jour dans le cadre de la mise à jour de l'agent. Cela permet d'empêcher le système automatisé d'écraser une action effectuée par un administrateur.

Lorsque vous testez des mises à jour d'agent, tenez compte des points suivants :

- BlackBerry recommande de tester les règles de mise à jour de l'agent à l'aide de règles de mise à jour et de zones créées à des fins de test (par exemple, à l'aide des règles de mise à jour Test et Pilote) avant d'utiliser d'autres règles de mise à jour que vous avez ajoutées pour le déploiement en production. Lors du test des mises à jour, pensez à utiliser des terminaux réservés à des fins de test et d'évaluation.
- Créez des zones pour tester les mises à jour des agents et ajoutez des terminaux qui sont réservés au test. Associez les zones que vous avez créées aux règles de mise à jour Test et Pilote. Pour en savoir plus sur la création de zones, reportez-vous à Configurer les zones pour gérer CylancePROTECT Desktop et CylanceOPTICS.
- Assurez-vous que tous les terminaux de test se trouvent dans une zone que vous testez. La règle de mise à jour Production s'applique à tous les terminaux qui ne se trouvent pas dans une zone à laquelle est associée une autre règle de mise à jour.

**Remarque :** Si la protection de la mémoire, le contrôle des scripts et/ou le contrôle du terminal sont activés dans la stratégie de terminal, un redémarrage du terminal après l'installation ou la mise à niveau de l'agent est recommandé, mais pas strictement requis. Un redémarrage permet de s'assurer que tous les nouveaux paramètres de stratégie sont pleinement pris en compte.

#### Fonctionnement des règles de mise à jour avec les zones

- Les terminaux sont associés à des zones par le biais de règles de zone ou par affectation manuelle.
- Les terminaux peuvent être associés à plusieurs zones.
- Les zones sont affectées aux règles de mise à jour. Les terminaux affectés à ces zones suivront les règles de mise à jour.
- Les règles de mise à jour ne sont pas spécifiques à une plateforme de système d'exploitation, mais vous pouvez créer des zones pour gérer les mises à jour des terminaux avec des plateformes de système d'exploitation spécifiques. Si la version de l'agent spécifiée dans la règle de mise à jour n'est pas disponible pour une plateforme, le terminal reçoit la mise à jour dès qu'elle devient disponible pour la plateforme.
- Les règles de mise à jour sont classées. Si un terminal est associé à plusieurs zones auxquelles des règles de mise à jour différentes sont attribuées, la règle de mise à jour la mieux classée qui spécifie une mise à jour pour l'agent (mise à jour automatique ou version spécifique) prend effet. Si un terminal se trouve dans

au moins une zone dans laquelle une règle de mise à jour spécifie une mise à jour, l'agent sur le terminal sera mis à jour en conséquence. La règle de mise à jour de production a le rang le plus bas et s'applique aux terminaux qui ne se trouvent dans aucune zone comportant une règle de mise à jour, et aux terminaux qui se trouvent dans les zones où aucune des règles n'a spécifié de mise à jour pour l'agent.

#### Exemples de règles de mise à jour

Les exemples suivants illustrent des règles de mise à jour auxquelles sont affectées des zones créées spécifiquement pour les mises à jour par zone.

| Exemple de règle de mise à jour | Zones affectées |
|---|---|
| Windows Serveur : Test | • Windows Serveur : zone de mise à jour Test aux États-Unis<br>• Windows Serveur : zone de mise à jour Test en Europe |
| Windows Serveur : Pilote | • Windows Serveur : zone de mise à jour Pilote aux États-Unis<br>• Windows Serveur : zone de mise à jour Pilote en Europe |
| Windows Serveur : Production | • Windows Serveur : zone de mise à jour Production aux États-Unis<br>• Windows Serveur : zone de mise à jour Production en Europe |

# Gérer les mises à jour pour les agents CylancePROTECT Desktop et CylanceOPTICS

**Avant de commencer :** Vous devez créer des zones avec des terminaux réservés aux tests des mises à jour d'agent. Vous associerez ces zones aux règles de mise à jour Test et Pilot. Vous pouvez ajouter vos propres règles de mise à jour pour réaliser des tests ou pour un déploiement de production. Pour en savoir plus sur la création de zones, reportez-vous à Configurer les zones pour gérer CylancePROTECT Desktop et CylanceOPTICS.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Mettre à jour**.
2. Si nécessaire, créez une règle de mise à jour. Par exemple, vous pouvez créer une règle pour tester les mises à jour de l'agent.
   a) Cliquez sur **Ajouter une nouvelle règle**.
   b) Saisissez un nom pour la règle.
   c) Cliquez sur **Envoyer**.
3. Cliquez sur une règle de mise à jour. Par exemple, cliquez sur **Test**.
4. Développez **Zones** et sélectionnez les zones que vous souhaitez attribuer à cette règle de mise à jour.
5. Développez **Agent** et sélectionnez une option de mise à jour.

   **Remarque :** Si vous ne souhaitez pas mettre à jour la version de l'agent sur un terminal, utilisez le paramètre **Ne pas mettre à jour**. Vous devez également vous assurer que le terminal ne se trouve pas dans une autre zone avec une autre règle de mise à jour (y compris la règle de production) qui spécifie une mise à jour de l'agent (mise à jour automatique ou version spécifique). Si un terminal se trouve dans une zone qui comporte une règle de mise à jour spécifiant une mise à jour, il sera mis à jour. Si un terminal est associé à plusieurs règles de mise à jour qui spécifient une mise à jour, l'agent est mis à jour en fonction de la règle ayant le rang le plus élevé.
6. Cochez la case **Mise à jour automatique du pilote Linux** pour permettre à l'agent de se mettre automatiquement à jour vers le dernier pilote pour prendre en charge le dernier kernel Linux. La fonctionnalité

de mise à jour automatique du pilote Linux nécessite l'agent CylancePROTECT Desktop 3.1.1000 ou ultérieure et le pilote de l'agent version 3.1.1000 ou ultérieure.

7. Développez **CylanceOPTICS** et sélectionnez une option de mise à jour.

   Vous pouvez sélectionner Mise à jour automatique uniquement si vous avez configuré l'agent CylancePROTECT Desktop pour utiliser la mise à jour automatique.
8. Répétez les étapes 2 à 7 pour la règle de mise à jour du **Pilote** ou une règle que vous avez créée pour le test pilote.
9. Répétez les étapes 2 à 7 pour la règle de mise à jour de **Production** ou une règle que vous avez créée pour la production. Vous n'affectez pas de zones à la règle de mise à jour de **Production** par défaut, car elle s'applique à tous les terminaux qui ne sont pas dans une zone comportant une règle de mise à jour.

   Si l'agent CylancePROTECT Desktop est défini sur Mise à jour automatique dans la règle de mise à jour Production, les règles Test et Pilote ne sont pas disponibles. Les règles de mise à jour que vous créez ne sont pas affectées par la configuration de la règle de mise à jour Production.
10. Cliquez sur **Enregistrer**.

**À la fin :**

- Si vous avez ajouté des règles de mise à jour, cliquez sur les flèches près des règles pour définir le classement. Les règles figurant en haut de la liste sont prioritaires sur celles situées plus bas dans la liste. Les règles Test, Pilot et Production sont toujours situées au bas de la liste et vous ne pouvez pas modifier leur classement. La règle de mise à jour de production est appliquée aux terminaux qui ne se trouvent dans aucune zone comportant une règle de mise à jour, et aux terminaux qui se trouvent dans des zones où aucune des règles n'a spécifié de mise à jour pour l'agent.
- Pour déclencher une mise à jour de l'agent CylancePROTECT Desktop avant l'intervalle horaire sur un terminal, cliquez avec le bouton droit de la souris sur l'icône CylancePROTECT Desktop dans la barre d'état système du terminal et cliquez sur **Rechercher des mises à jour**, redémarrez le service Cylance ou exécutez la commande suivante à partir du répertoire Cylance :

  ```
  CylanceUI.exe–update
  ```
- Si la protection de la mémoire, le contrôle des scripts et/ou le contrôle du terminal sont activés dans la stratégie de terminal, un redémarrage du terminal après l'installation ou la mise à niveau de l'agent est recommandé, mais pas strictement requis. Un redémarrage permet de s'assurer que tous les nouveaux paramètres de stratégie sont pleinement pris en compte.

# Connexion de Cylance Endpoint Security à des services externes

Cylance Endpoint Security prend en charge différents connecteurs qui vous permettent d'intégrer des données et des fonctionnalités à des services tiers et à d'autres produits BlackBerry. Un locataire Cylance Endpoint Security peut se connecter à plusieurs services externes.

Cylance Endpoint Security prend en charge les connecteurs suivants :

| Connecteur | Description |
|---|---|
| BlackBerry UEM | Le connecteur BlackBerry UEM permet à CylanceGATEWAY de vérifier si les terminaux Android et iOS sont gérés par UEM.<br><br>Pour plus d'informations, reportez-vous à Connexion de Cylance Endpoint Security aux solutions MDM pour vérifier si les terminaux sont gérés. |
| Microsoft Intune | Le connecteur Microsoft Intune Cylance Endpoint Security permet de signaler le niveau de risque des terminaux mobiles de votre organisation gérés par Intune. Le niveau de risque du terminal est calculé en fonction de la détection des menaces mobiles par l'application CylancePROTECT Mobile sur les terminaux gérés par Intune. Intune peut exécuter des actions d'atténuation en fonction du niveau de risque du terminal.<br><br>Pour plus d'informations, reportez-vous à Intégration d'Cylance Endpoint Security à Microsoft Intune pour répondre aux menaces mobiles. |
| Okta | Le connecteur Okta vous permet de collecter des informations d'authentification de connexion et d'accès à partir des services Okta, ainsi que d'afficher les informations connexes dans la vue Alertes de la console Cylance.<br><br>Pour plus d'informations, reportez-vous à Intégration de Cylance Endpoint Security avec Okta. |
| Mimecast | Le connecteur Mimecast vous permet d'intégrer les données de valeur de risque relatives aux pièces jointes à partir des services Mimecast, ainsi que d'afficher les informations connexes dans la vue Alertes de la console Cylance.<br><br>Pour plus d'informations, reportez-vous à Intégration de Cylance Endpoint Security avec Mimecast. |

## Intégration de Cylance Endpoint Security avec Okta

Vous pouvez ajouter une connexion Okta à votre console Cylance pour afficher les alertes Okta dans la vue Alertes. La vue Alertes permet aux administrateurs d'afficher les alertes d'autorisation et d'accès Okta à partir d'une interface unifiée. Le connecteur Okta utilise l'API d'évènements Okta pour afficher la télémétrie des évènements dans la vue Alertes. Les évènements d'anomalie d'utilisateur Okta agrégés dans la vue Alertes incluent les tentatives de connexion utilisateur suspectes et les évènements de demandes de sécurité bloquées. En regroupant les évènements Okta dans ces catégories, vous bénéficiez d'une plus grande visibilité sur les tentatives de connexion de tiers, les connexions erronées des utilisateurs et les tentatives de connexion d'adresses IP sources suspectes.

La vue Alertes regroupe les demandes provenant d'adresses IP interdites dans la base d'utilisateurs de votre entreprise afin de fournir des informations sur les modèles ou campagnes possibles. Les données affichées peuvent également contenir des informations sur le terminal source de la tentative d'accès, ce qui vous permet de déterminer si la demande provient d'un humain ou d'une machine.

Pour plus d'informations sur la configuration de Okta pour générer des alertes à afficher dans la vue Alertes, consultez les ressources suivantes :

- Okta Help Center: Configure a password policy
- Okta Help Center: Blocklist network zones

Pour plus d'informations sur la vue Alertes, reportez-vous à la section Gestion des alertes sur les services Cylance Endpoint Security dans le contenu relatif à l'administration.

### Conditions préalables pour l'ajout d'un connecteur Okta

Avant de pouvoir configurer une connexion Okta pour Cylance Endpoint Security, vous devez effectuer certaines tâches à l'aide du service Okta.

| Étape | Élément | Description |
|---|---|---|
| 1 | Documenter l'URL de base Okta | Vous devez documenter l'URL de base Okta de votre environnement pour l'utiliser lors de la configuration du connecteur Okta. L'URL de base Okta correspond à l'URL de production de votre serveur Okta.<br><br>Pour en savoir plus sur la localisation de votre URL de base Okta, consultez la section Find your Okta Domain dans la documentation Okta. |
| 2 | Créer un administrateur Okta | Vous devez créer un administrateur Okta pour utiliser l'API Okta. BlackBerry recommande de créer un utilisateur dédié lié au jeton d'API à l'étape 3. Cette étape est recommandée, car elle facilite l'audit des flux de travail et permet d'éviter que les autres utilisateurs de Okta créent des jetons et les utilisent dans les flux d'opérations de sécurité.<br><br>Pour en savoir plus sur la création d'un administrateur Okta, consultez la section Create an admin role assignment using an admin dans la documentation Okta. |
| 3 | Créer un jeton d'API Okta | Vous devez créer un jeton d'API Okta pour authentifier les demandes auprès de l'API Okta.<br><br>Pour en savoir plus sur la création d'un jeton d'API Okta, consultez la section API token management dans la documentation Okta. |

Après avoir effectué ces étapes, suivez les instructions de la section Ajouter et configurer un connecteur Okta.

### Ajouter et configurer un connecteur Okta

**Avant de commencer :** Examinez Conditions préalables pour l'ajout d'un connecteur Okta.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Connecteurs**.

2. Cliquez sur **Ajouter un connecteur > Okta**.
3. Dans la section **Informations générales**, saisissez un nom pour le connecteur.
4. Dans la section **Configuration d'Okta**, spécifiez l'URL de l'API de service Okta, le jeton d'API Okta et la fréquence d'interrogation.

   **Remarque :** BlackBerry recommande de conserver la valeur par défaut de la fréquence d'interrogation, sauf si votre organisation a défini une valeur seuil spécifique.
5. Cliquez sur **Test de connexion**.
6. Cliquez sur **Enregistrer**.

**À la fin :** Affichez et gérez les alertes dans la vue Alertes. Reportez-vous à la section Gestion des alertes sur les services Cylance Endpoint Security dans le contenu relatif à l'administration.

# Intégration de Cylance Endpoint Security avec Mimecast

Vous pouvez ajouter un connecteur Mimecast à votre console Cylance. La protection des pièces jointes Mimecast analyse toutes les pièces jointes que vos utilisateurs reçoivent et peut les gérer en fonction de la stratégie que vous configurez.

La vue Alertes permet aux administrateurs d'afficher les informations sur les risques liés aux pièces jointes Mimecast à partir d'une interface unifiée. Mimecast affiche la télémétrie des risques liés aux pièces jointes fournie par le service Sécurité avancée des e-mails de Mimecast. L'action que Mimecast applique à la pièce jointe s'affiche dans la colonne de réponse de la vue Alertes. Si Mimecast classe une alerte comme malveillante, elle sera hiérarchisée dans la catégorie de priorité élevée dans la vue Alertes. Si Mimecast classe une alerte comme non sécurisée ou inconnue, elle sera hiérarchisée dans la catégorie de priorité moyenne. Toutes les alertes considérées comme de priorité faible par Mimecast ne s'affichent pas dans la vue Alertes.

La vue Alertes utilise le hachage de pièce jointe pour regrouper les alertes, ce qui signifie qu'une alerte similaire affectant plusieurs utilisateurs de votre organisation peut être groupée pour la même menace. Vous pouvez utiliser le lien Détails de la détection pour accéder au tableau de bord Protection des pièces jointes Mimecast afin d'étudier les menaces et de les corriger.

Pour plus d'informations sur la vue Alertes, reportez-vous à la section Gestion des alertes sur les services Cylance Endpoint Security dans le contenu relatif à l'administration.

## Conditions préalables pour l'ajout d'un connecteur Mimecast

Avant de pouvoir configurer une connexion Mimecast pour Cylance Endpoint Security, vous devez effectuer certaines tâches à l'aide du service Mimecast.

| Étape | Tâche | Détails |
|---|---|---|
| 1 | Créer un compte Mimecast | Les administrateurs doivent créer un nouveau compte pour tous les utilisateurs du service.<br>Pour en savoir plus, consultez la section Création/modification d'utilisateurs Mimecast dans la documentation Mimecast. |

| Étape | Tâche | Détails |
|---|---|---|
| 2 | Ajouter une application d'API | Spécifiez les détails et les paramètres de votre application d'API. Lors de la configuration de l'application API, vérifiez que Application de service est sélectionné. Cela est nécessaire pour garantir que les clés API n'expirent pas. Si cette option n'est pas sélectionnée, le connecteur Mimecast perd la connectivité lorsque la clé expire.<br>Pour en savoir plus sur l'ajout d'une application d'API dans Mimecast, consultez la section Ajout d'une application d'API dans le guide Gestion des applications d'API de Mimecast. |
| 3 | Créer des clés d'association d'utilisateur | Vous devez créer des clés d'association d'utilisateur pour connecter Mimecast à Cylance Endpoint Security.<br>Pour en savoir plus sur la création de clés d'association d'utilisateur, consultez la section Création de clés d'association d'utilisateur dans le guide Gestion des applications d'API de Mimecast. |
| 4 | Informer les utilisateurs de la configuration Mimecast | Il est recommandé d'informer vos utilisateurs de la configuration Mimecast. Vous pouvez télécharger les modèles d'e-mail préconfigurés disponibles sur Mimecast. |
| 5 | Configurer les définitions et les stratégies de protection des pièces jointes | Configurez les définitions et les stratégies de protection des pièces jointes que Mimecast utilise lors de la détection d'un e-mail non sécurisé.<br>Pour en savoir plus, consultez la section Configuration de la protection des pièces jointes dans la documentation Mimecast. |
| 6 | Activer et configurer les notifications | Assurez-vous d'avoir activé et configuré les notifications pour tous les utilisateurs de l'API afin qu'elles soient disponibles dans la vue Alertes.<br>Pour en savoir plus, consultez la section Configuration de la protection des pièces jointes dans la documentation Mimecast. |

| Étape | Tâche | Détails |
|---|---|---|
| 7 | Activer les services d'annuaire | Assurez-vous d'avoir activé les services d'annuaire Mimecast afin de corréler les informations utilisateur (adresse e-mail) Mimecast avec vos données utilisateur stockées dans votre service Entra ou Active Directory. Cette configuration permet également la corrélation avec vos terminaux et les données de terminal associées aux utilisateurs de vos services d'annuaire.<br><br>Pour plus d'informations sur l'activation des services d'annuaire, reportez-vous à la section Synchronisation d'annuaire dans la documentation Mimecast. |

Après avoir effectué ces étapes, suivez les instructions de la section Ajouter et configurer un connecteur Mimecast.

### Ajouter et configurer un connecteur Mimecast

**Avant de commencer :** Examinez Conditions préalables pour l'ajout d'un connecteur Mimecast.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Connecteurs**.
2. Cliquez sur **Ajouter un connecteur > Mimecast**.
3. Dans la section **Informations générales**, saisissez un nom pour le connecteur.
4. Dans la section **Configuration Mimecast**, spécifiez les informations requises, indiquez une fréquence d'interrogation et sélectionnez une URL de base.

   Pour en savoir plus sur la génération de clés Mimecast, consultez la section Gestion des applications API dans la documentation Mimecast.
5. Cliquez sur le bouton bascule pour activer l'interrogation.
6. Cliquez sur **Test de connexion**.
7. Cliquez sur **Enregistrer**.

**À la fin :** Affichez et gérez les alertes dans la vue Alertes. Reportez-vous à la section Gestion des alertes sur les services Cylance Endpoint Security dans le contenu relatif à l'administration.

# Annexe : bonnes pratiques pour le déploiement de CylancePROTECT Desktop sur des machines virtuelles Windows

Vous pouvez utiliser CylancePROTECT Desktop pour protéger à la fois des machines physiques et virtuelles. Cette section décrit les bonnes pratiques de déploiement de l'agent CylancePROTECT Desktop sur des postes de travail VDI (Virtual Desktop Infrastructure) basés sur Windows.

CylancePROTECT Desktop fonctionne bien en tant que composant du système d'exploitation invité, car il n'est pas gourmand en opérations d'E/S par seconde ou en mémoire par invité. La préparation et le déploiement de l'agent CylancePROTECT Desktop dans un environnement virtuel sont similaires à ceux d'un déploiement sur un ordinateur physique. Les étapes de déploiement et les bonnes pratiques de cette section garantissent que l'agent fonctionne efficacement dans un environnement virtuel avec moins de ressources allouées et vous aideront à produire une image de référence sans fichiers dangereux ou anormaux. Lorsque l'image de référence a été soigneusement approuvée, il est possible de cloner les images VDI de production à partir de celle-ci.

## Configuration requise et considérations relatives à l'utilisation de CylancePROTECT Desktop sur des machines virtuelles

| Élément | Configuration requise ou considérations |
| --- | --- |
| Technologies de virtualisation Enterprise prises en charge | • Microsoft Hyper-V<br>• Citrix XenDesktop<br>• VMware Horizon/View<br>• VMware Workstation<br>• VMware Fusion |

| Élément | Configuration requise ou considérations |
| --- | --- |
| Machines virtuelles non persistantes | Une machine virtuelle non persistante est supprimée à la fin de la session et remplacée par la même image de référence. Lorsqu'une nouvelle machine virtuelle est créée, l'agent CylancePROTECT Desktop enregistre la machine virtuelle auprès de la console de gestion, ce qui entraîne l'enregistrement de terminaux en double pour ce qui doit être le même point de terminaison (les enregistrements plus anciens sont traités comme des enregistrements de terminaux hors ligne en double qui ne reviennent jamais en ligne).<br><br>Utilisez l'un des paramètres d'installation suivants lorsque vous installez l'agent CylancePROTECT Desktop sur l'image de référence afin d'éviter la duplication de l'enregistrement du même terminal de machine virtuelle :<br><br>• `VDI=<X>` : la valeur de `<X>` est un compteur qui détermine le moment où l'agent commence à identifier la machine virtuelle à l'aide de l'empreinte VDI au lieu du mécanisme d'empreinte digitale de l'agent par défaut. Les terminaux en double ne sont pas enregistrés lorsque l'agent utilise l'empreinte VDI.<br>  • Par exemple, vous installez l'agent sur une image de référence à l'aide du paramètre `VDI=2`. Vous utilisez l'image de référence pour créer une image parente. Vous pouvez ensuite utiliser l'image parente pour créer une image de poste de travail. L'agent commence à utiliser l'empreinte VDI pour l'image du poste de travail, car le compteur de 2 a été atteint par l'image de référence et l'image parente.<br>• `AD=1` : ce paramètre fonctionne de la même manière que `VDI=<X>`, sauf qu'il n'y a pas de compteur pour définir à quel moment l'agent commence à utiliser l'empreinte VDI. L'agent utilisera l'empreinte VDI sur l'image de référence et pour toutes les images que vous créez à partir de celle-ci. Ce paramètre n'est pas pris en charge pour le format .exe du programme d'installation unifié CylancePROTECT Desktop et CylanceOPTICS. |
| Fonctionnalités de protection de la mémoire et de contrôle des scripts | Tenez compte des points suivants avant d'activer les fonctionnalités de protection de la mémoire et de contrôle des scripts dans un environnement VDI :<br><br>• Les deux fonctionnalités utilisent l'injection de processus pour identifier et bloquer le code indésirable ou non autorisé. Les plug-ins, les outils ou les DLL dans les environnements virtualisés peuvent avoir des effets négatifs. Vous devez donc tester les options de protection de la mémoire et de contrôle des scripts avant de les déployer sur les postes de travail de production.<br>• Il est recommandé de tester les options de protection de la mémoire en mode alerte uniquement et y apporter des modifications de stratégie de terminal plus strictes. Si le système devient instable, vous pouvez désactiver la protection de la mémoire.<br>• En cas de conflits ou d'instabilités du système, en tant qu'option de sécurité intégrée, vous pouvez activer le mode de compatibilité pour la protection de la mémoire.<br>• Reportez-vous à la section Incompatibilités connues pour la protection de la mémoire et le contrôle des scripts v2 dans Protect 1580 et les versions ultérieures. |

| Élément | Configuration requise ou considérations |
|---|---|
| Option permettant de désactiver l'interface utilisateur de l'agent | Vous avez la possibilité de désactiver l'interface utilisateur de l'agent CylancePROTECT Desktop pour préserver l'ensemble des ressources système. Pour plus d'informations, reportez-vous à Paramètres d'installation Windows. |
| Problèmes connus | Pour examiner les problèmes signalés lors de l'exécution de l'agent CylancePROTECT Desktop dans un environnement virtuel, reportez-vous à la section Problèmes de tendance VDI. |

# Déployer CylancePROTECT Desktop sur des machines virtuelles

**Avant de commencer :** Examinez Configuration requise et considérations relatives à l'utilisation de CylancePROTECT Desktop sur des machines virtuelles.

1. Créez une stratégie de terminal que vous utiliserez pour préparer l'image de référence VDI. Configurez les options suivantes dans la stratégie :

   | Catégorie de stratégie de terminal | Options |
   |---|---|
   | Actions de fichier | Activer **Mise en quarantaine automatique avec contrôle d'exécution** pour les types de fichiers dangereux et anormaux |
   | Paramètres de protection | • Activer la **Détection des menaces en arrière-plan** (**Exécuter une fois**)<br>• Activer **Contrôler les nouveaux fichiers** |

2. Préparez l'image VDI de référence.
   a) Installer l'agent CylancePROTECT Desktop sur l'image de référence. Par exemple, utilisez la commande et les paramètres d'installation suivants :

   ```
   msiexec /i CylancePROTECTSetup_x64.msi /qn PIDKEY=<INSTALLATION TOKEN> VDI=1
    LAUNCHAPP=1
   ```

   b) Appliquez la stratégie de terminal que vous avez créée à l'étape 1 à l'image de référence.

   Laissez l'analyse de détection des menaces en arrière-plan se terminer. Ceci peut nécessiter plusieurs heures, selon la taille du disque et l'activité sur l'image au cours de l'analyse.

   c) Passez en revue les résultats de l'analyse de détection des menaces en arrière-plan et, si nécessaire, ajoutez des fichiers binaires détectés sur l'image de référence aux listes de quarantaine ou sécurisée CylancePROTECT Desktop.
3. Sur l'image de référence, effacez les valeurs d'empreinte du registre.
   a) Arrêtez le service CylanceSvc. Rendez-vous sur support.blackberry.com pour consulter l'article KB 107236.
   b) À l'aide du compte d'administrateur local, prenez possession de la clé de registre et ajoutez des autorisations de contrôle complet au registre suivant : `HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop`
   c) Sauvegardez ou exportez le registre indiqué ci-dessus.
   d) Supprimez les clés de registre suivantes : FP, FPMask et FPversion.
4. Créez l'image de référence.

5. Créez une stratégie de terminal destinée aux postes de travail VDI de production. BlackBerry recommande les options suivantes dans la stratégie, en plus des options que vous souhaitez activer pour vos postes de travail de production :

| Catégorie de stratégie de terminal | Options |
|---|---|
| Actions de fichier | • Activer **Mise en quarantaine automatique avec contrôle d'exécution** pour les types de fichiers dangereux et anormaux<br>• Activer le **Chargement automatique** |
| Paramètres de protection | • Activer **Contrôler les nouveaux fichiers**<br>• Désactiver la **Détection des menaces en arrière-plan** |

6. Déployez et clonez l'image de référence sur les postes de travail de production. Chaque image clonée doit disposer d'un UUID ou ID unique différent de l'image de référence.
7. Appliquez la stratégie de terminal de l'étape 5 aux postes de travail de production.

**À la fin :** Pour les terminaux clonés, configurez les mises à jour de l'agent basé sur la zone sur **Ne pas mettre à jour** ou sur une version spécifique de l'agent. Les mises à jour doivent être gérées sur l'image de référence. Reportez-vous à la section Mettre à jour CylancePROTECT Desktop sur des terminaux clonés.

# Mettre à jour CylancePROTECT Desktop sur des terminaux clonés

**Avant de commencer :** Déployer CylancePROTECT Desktop sur des machines virtuelles.

1. Sur l'image de référence, mettez à jour l'agent CylancePROTECT Desktop.
2. Si des mises à jour ou des fichiers supplémentaires sont appliqués à l'image de référence, appliquez la règle de terminal de préparation VDI à l'image de référence et laissez l'analyse de détection des menaces en arrière-plan se terminer.
3. Passez en revue les résultats de l'analyse de détection des menaces en arrière-plan et, si nécessaire, ajoutez des fichiers binaires détectés sur l'image de référence aux listes de quarantaine ou sécurisée CylancePROTECT Desktop.
4. Appliquez la stratégie de terminal de production à l'image de référence.
5. Scellez à nouveau l'image de référence.
6. Vérifiez que la mise à jour de l'agent a été propagée aux terminaux clonés.

# Informations juridiques



Cette documentation, y compris la documentation incluse pour référence telle que celle fournie ou mise à disposition sur le site Web BlackBerry, est fournie ou mise à disposition « EN L'ÉTAT » et « TELLE QUELLE », sans condition ni garantie en tout genre de la part de BlackBerry Limited et de ses filiales (« BlackBerry »), et BlackBerry décline toute responsabilité en cas d'erreur ou d'oubli typographique, technique ou autre inexactitude contenue dans ce document. Pour des raisons de protection des informations confidentielles et/ou des secrets commerciaux de BlackBerry, cette documentation peut décrire certains aspects de la technologie BlackBerry en termes généraux. BlackBerry se réserve le droit de modifier périodiquement les informations contenues dans cette documentation. Cependant, BlackBerry ne s'engage en aucune manière à vous communiquer les modifications, mises à jour, améliorations ou autres ajouts apportés à cette documentation.

La présente documentation peut contenir des références à des sources d'informations, du matériel ou des logiciels, des produits ou des services tiers, y compris des composants et du contenu tel que du contenu protégé par copyright et/ou des sites Web tiers (ci-après dénommés collectivement « Produits et Services tiers »). BlackBerry ne contrôle pas et décline toute responsabilité concernant les Produits et Services tiers, y compris, sans s'y limiter, le contenu, la précision, le respect du code de la propriété intellectuelle, la compatibilité, les performances, la fiabilité, la légalité, l'éthique, les liens ou tout autre aspect desdits Produits et Services tiers. La présence d'une référence aux Produits et Services tiers dans cette documentation ne suppose aucunement que BlackBerry se porte garant des Produits et Services tiers ou de la tierce partie concernée.

SAUF DANS LA MESURE SPÉCIFIQUEMENT INTERDITE PAR LES LOIS EN VIGUEUR DANS VOTRE JURIDICTION, TOUTES LES CONDITIONS, GARANTIES OU REPRÉSENTATIONS DE TOUTE NATURE, EXPRESSES OU TACITES, NOTAMMENT (SANS LIMITATIONS) LES CONDITIONS, GARANTIES OU REPRÉSENTATIONS DE DURABILITÉ, D'ADÉQUATION À UNE UTILISATION OU À UN BUT PARTICULIER, DE COMMERCIALISATION, DE QUALITÉ MARCHANDE, DE NON-INFRACTION, DE SATISFACTION DE LA QUALITÉ OU DE TITRE, OU RÉSULTANT D'UNE LOI, D'UNE COUTUME, D'UNE PRATIQUE OU D'UN USAGE COMMERCIAL, OU EN RELATION AVEC LA DOCUMENTATION OU SON UTILISATION, OU LA PERFORMANCE OU NON-PERFORMANCE DES LOGICIELS, DU MATÉRIEL, DES SERVICE OU DES PRODUITS ET SERVICES TIERS CITÉS, SONT EXCLUES. VOUS POUVEZ JOUIR D'AUTRES DROITS QUI VARIENT SELON L'ÉTAT OU LA PROVINCE. CERTAINES JURIDICTIONS N'AUTORISENT PAS L'EXCLUSION OU LA LIMITATION DES GARANTIES ET CONDITIONS IMPLICITES. DANS LA MESURE AUTORISÉE PAR LES LOIS, TOUTE GARANTIE OU CONDITION IMPLICITE RELATIVE À LA DOCUMENTATION, DANS LA MESURE OÙ ELLES NE PEUVENT PAS ÊTRE EXCLUES EN VERTU DES CLAUSES PRÉCÉDENTES, MAIS PEUVENT ÊTRE LIMITÉES, SONT PAR LES PRÉSENTES LIMITÉES À QUATRE-VINGT-DIX (90) JOURS À COMPTER DE LA DATE DE LA PREMIÈRE ACQUISITION DE LA DOCUMENTATION OU DE L'ARTICLE QUI FAIT L'OBJET D'UNE RÉCLAMATION.

DANS LA MESURE MAXIMALE PERMISE PAR LES LOIS EN VIGUEUR DANS VOTRE JURIDICTION, EN AUCUN CAS BLACKBERRY N'EST RESPONSABLE DES DOMMAGES LIÉS À LA PRÉSENTE DOCUMENTATION OU À SON UTILISATION, OU À LA PERFORMANCE OU NON-PERFORMANCE DES LOGICIELS, DU MATÉRIEL, DES SERVICES OU DES PRODUITS ET SERVICES TIERS MENTIONNÉS DANS LES PRÉSENTES, ET NOTAMMENT, SANS S'Y LIMITER, DES DOMMAGES DIRECTS, EXEMPLAIRES, ACCIDENTELS, INDIRECTS, SPÉCIAUX, PUNITIFS OU AGGRAVÉS, DES DOMMAGES LIÉS À UNE PERTE DE PROFITS OU DE REVENUS, UN MANQUE À GAGNER, UNE INTERRUPTION D'ACTIVITÉ, UNE PERTE D'INFORMATIONS COMMERCIALES, UNE PERTE D'OPPORTUNITÉS COMMERCIALES, LA CORRUPTION OU LA PERTE DE DONNÉES, LE NON-ENVOI OU LA NON-RÉCEPTION DE DONNÉES, DES PROBLÈMES LIÉS À DES APPLICATIONS UTILISÉES AVEC DES PRODUITS OU SERVICES BLACKBERRY, DES COUTS D'INDISPONIBILITÉ, LA PERTE D'UTILISATION DES PRODUITS OU SERVICES BLACKBERRY EN TOUT OU EN PARTIE, OU DE TOUT SERVICE DE COMMUNICATION, DU COUT DE BIENS DE

SUBSTITUTION, DES FRAIS DE GARANTIE, DES ÉQUIPEMENTS OU SERVICES, DES COUTS DE CAPITAL, OU AUTRES PERTES FINANCIÈRES SIMILAIRES, PRÉVISIBLES OU NON, MÊME SI BLACKBERRY A ÉTÉ INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES.

DANS LA MESURE MAXIMALE PERMISE PAR LES LOIS APPLICABLES DANS VOTRE JURIDICTION, BLACKBERRY N'EST NULLEMENT TENU PAR DES OBLIGATIONS, DEVOIRS OU RESPONSABILITÉS, CONTRACTUELS, DÉLICTUELS OU AUTRES, PAS MÊME PAR UNE RESPONSABILITÉ EN CAS DE NÉGLIGENCE OU RESPONSABILITÉ STRICTE ET NE VOUS EST REDEVABLE EN RIEN.

LES LIMITATIONS, EXCLUSIONS ET CLAUSES DE NON-RESPONSABILITÉ CONTENUES DANS LES PRÉSENTES S'APPLIQUENT : (A) INDÉPENDAMMENT DE LA NATURE DE LA CAUSE D'ACTION, DE DEMANDE OU D'ACTION ENTREPRISE PAR VOUS, NOTAMMENT, SANS S'Y LIMITER, POUR RUPTURE DE CONTRAT, NÉGLIGENCE, FAUTE, RESPONSABILITÉ STRICTE OU TOUTE AUTRE THÉORIE LÉGALE, ET RESTENT APPLICABLES EN CAS DE RUPTURES SUBSTANTIELLES OU DE MANQUEMENT AU BUT ESSENTIEL DU PRÉSENT CONTRAT OU DE TOUT RECOURS ENVISAGEABLE PAR LES PRÉSENTES ; ET (B) À BLACKBERRY ET À SES FILIALES, LEURS AYANTS DROIT, REPRÉSENTANTS, AGENTS, FOURNISSEURS (NOTAMMENT LES FOURNISSEURS DE SERVICES), REVENDEURS AGRÉÉS BLACKBERRY (NOTAMMENT LES FOURNISSEURS DE SERVICES) ET LEURS DIRECTEURS, EMPLOYÉS ET SOUS-TRAITANTS RESPECTIFS.

OUTRE LES LIMITATIONS ET EXCLUSIONS SUSMENTIONNÉES, EN AUCUN CAS, LES DIRECTEURS, EMPLOYÉS, AGENTS, REVENDEURS, FOURNISSEURS, SOUS-TRAITANTS DE BLACKBERRY OU DE SES FILIALES N'ONT UNE RESPONSABILITÉ CONSÉCUTIVE OU RELATIVE À LA PRÉSENTE DOCUMENTATION.

Avant de vous abonner, d'installer ou d'utiliser des Produits et Services tiers, il est de votre responsabilité de vérifier que votre fournisseur de services prend en charge toutes les fonctionnalités. Certains fournisseurs de services peuvent ne pas proposer de fonctionnalités de navigation Internet avec un abonnement à BlackBerry® Internet Service. Vérifiez auprès de votre fournisseur de services la disponibilité, les accords d'itinérance, les plans de service et les fonctionnalités. L'installation ou l'utilisation de Produits et Services tiers avec des produits et services BlackBerry peuvent nécessiter un ou plusieurs brevets, marques commerciales, licences de copyright ou autres licences à des fins de protection des droits d'autrui. Vous êtes seul responsable de votre décision d'utiliser ou non les Produits et Services tiers et si cela nécessite l'obtention de licences tierces. Si de telles licences sont requises, vous êtes seul responsable de leur acquisition. Vous ne devez pas installer ou utiliser de Produits et Services tiers avant d'avoir acquis la totalité des licences nécessaires. Les Produits et Services tiers fournis avec les produits et services BlackBerry vous sont fournis à toutes fins utiles « EN L'ÉTAT » sans conditions, garanties ou représentations expresses ou tacites d'aucune sorte par BlackBerry, et BlackBerry n'engage aucune responsabilité sur les Produits et Services tiers à cet égard. L'utilisation que vous faites des Produits et Services tiers est régie par et dépendante de votre acceptation des termes des licences et autres accords distincts applicables à cet égard avec d'autres parties, sauf dans la limite couverte expressément par une licence ou autre accord conclu avec BlackBerry.

Les conditions d'utilisation de tout produit ou service BlackBerry sont stipulées dans une licence ou autre accord distinct conclu avec BlackBerry à cet égard. LE CONTENU DE CETTE DOCUMENTATION N'EST PAS DESTINÉ À REMPLACER LES ACCORDS OU GARANTIES EXPRÈS ET ÉCRITS FOURNIS PAR BLACKBERRY POUR UNE PARTIE DES PRODUITS OU SERVICES BLACKBERRY AUTRES QUE CETTE DOCUMENTATION.

BlackBerry Enterprise Software incorpore des éléments logiciels tiers. La licence et les informations de copyright associées à ce logiciel sont disponibles à l'adresse http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited
2200 University Avenue Est
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,

Maidenhead, Berkshire SL6 1RL
Royaume-Uni

Publié au Canada