Configurer le déploiement de Microsoft Defender ATP

03/04/2020 • 6 minutes de lecture •

Dans cet article

S'applique à:

- Microsoft Defender– Protection avancée contre les menaces (MicrosoftDefender ATP)

Le déploiement de Microsoft Defender ATP est un processus en trois étapes:

Phase 1: préparation

Phase 2: configuration

Étape 3: intégration

Vous êtes actuellement dans la phase de configuration.

Dans ce scénario de déploiement, vous serez guidé dans les étapes suivantes:

- Validation de la gestion des licences
- Configuration du client
- Configuration du réseau

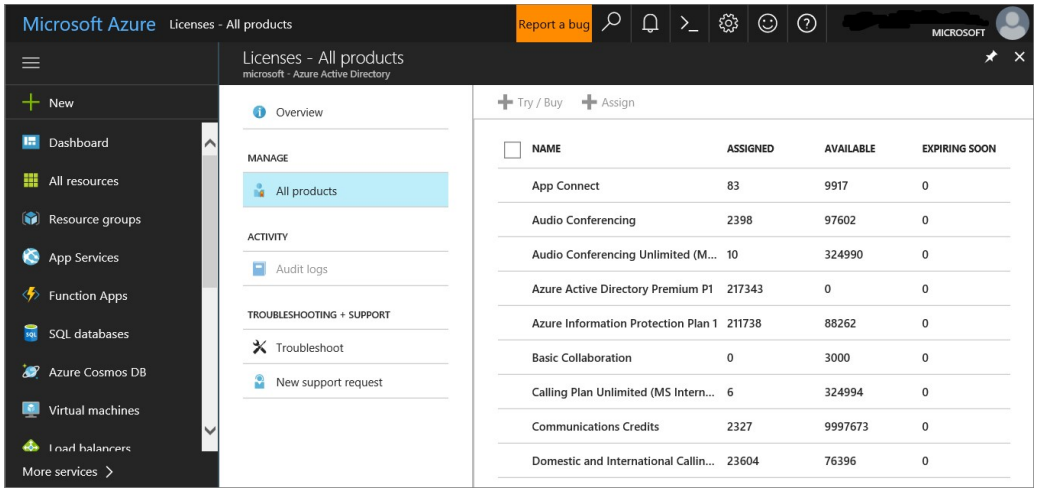
> **Notes**
>
> Pour vous guider dans le cadre d'un déploiement standard, ce scénario traite uniquement de l'utilisation du gestionnaire de configuration de point de terminaison Microsoft. Microsoft Defnder ATP prend en charge l'utilisation d'autres outils d'intégration, mais ne sera pas couvert par ces

scénarios dans le Guide de déploiement. Pour plus d'informations, reportez-vous à la rubrique [ordinateurs intégrés à Microsoft Defender ATP](#).

Vérifier l'état de la licence

La vérification de l'état de la licence et le mode de mise en service approprié peuvent être effectuées par le biais du centre d'administration ou du **portail Microsoft Azure**.

1. Pour afficher vos licences, accédez au **portail MicrosoftAzure**, puis naviguez jusqu'à la [section des licences du portail MicrosoftAzure](#).



2. Dans le centre d'administration, vous pouvez également accéder à la section**abonnements**de **facturation** > .

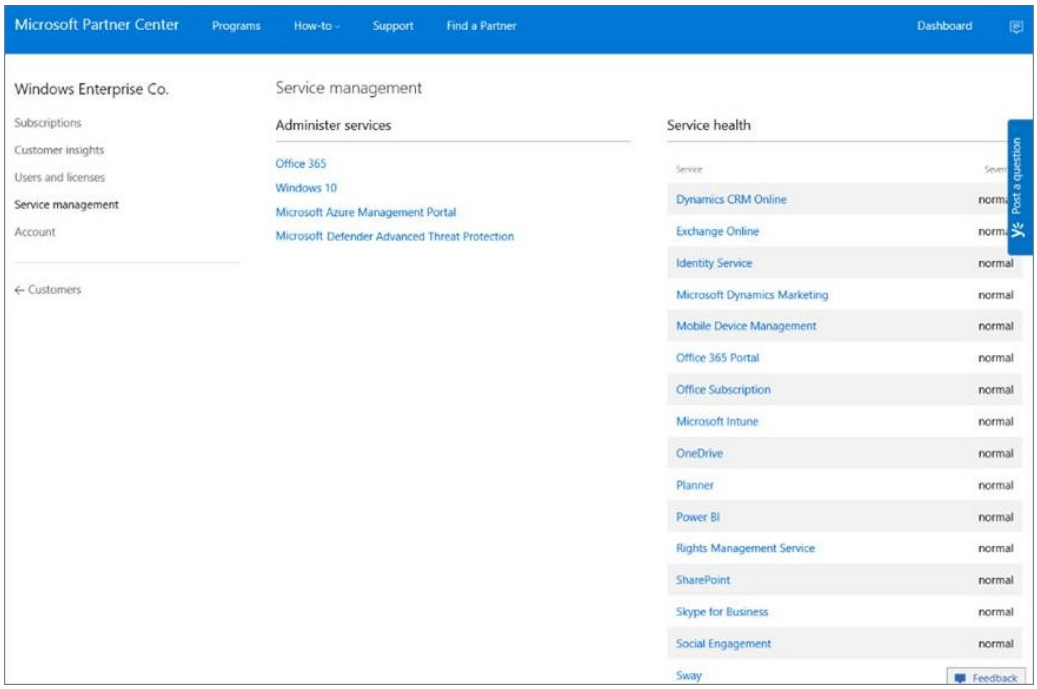
   Sur l'écran, vous verrez toutes les licences mises en service et leur **État** actuel.

Validation du fournisseur de services cloud

Pour vous permettre d'accéder aux licences configurées pour votre société et de vérifier l'état de celles-ci, accédez au centre d'administration.

1. Dans le **portail Partenaire**, cliquez sur **Administrer les services > Office365**.

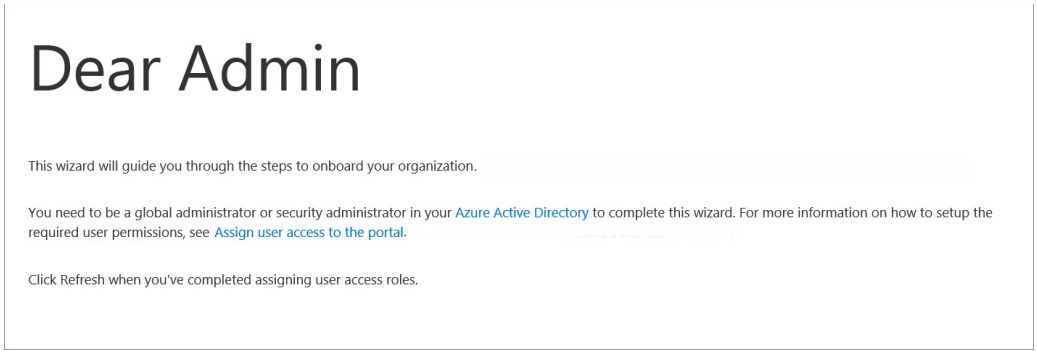
2. Cliquer sur le lien **portail du partenaire** utilisera l'option **administrateur de la part** de et vous donne accès au centre d'administration du client.



Configuration du client

Lorsque vous accédez au Centre de sécurité Microsoft Defender pour la première fois, un assistant de configuration vous guidera lors du processus initial. À la fin de l'Assistant Installation, une instance de Cloud dédiée de Microsoft Defender ATP est créée. La méthode la plus simple consiste à effectuer ces étapes à partir d'un ordinateur client Windows 10.

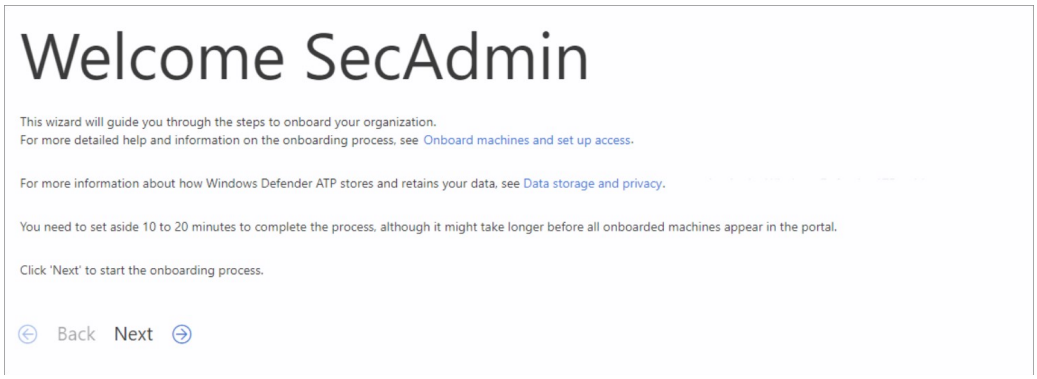
1. À partir d'un navigateur Web, https://securitycenter.windows.comaccédez à.



2. Si vous passez d'une licence d'évaluation, accédez au lien[https://signup.microsoft.com/Signup?OfferId=6033e4b5-c320-4008-a936-909c2825d83c&dl=WIN_DEF_ATP&pc=xxxxxxx-xxxxxx-xxx-x]().

   Une fois l'étape d'autorisation terminée, l'écran **Bienvenue** s'affiche.

3. Passez en revue les étapes d'autorisation.

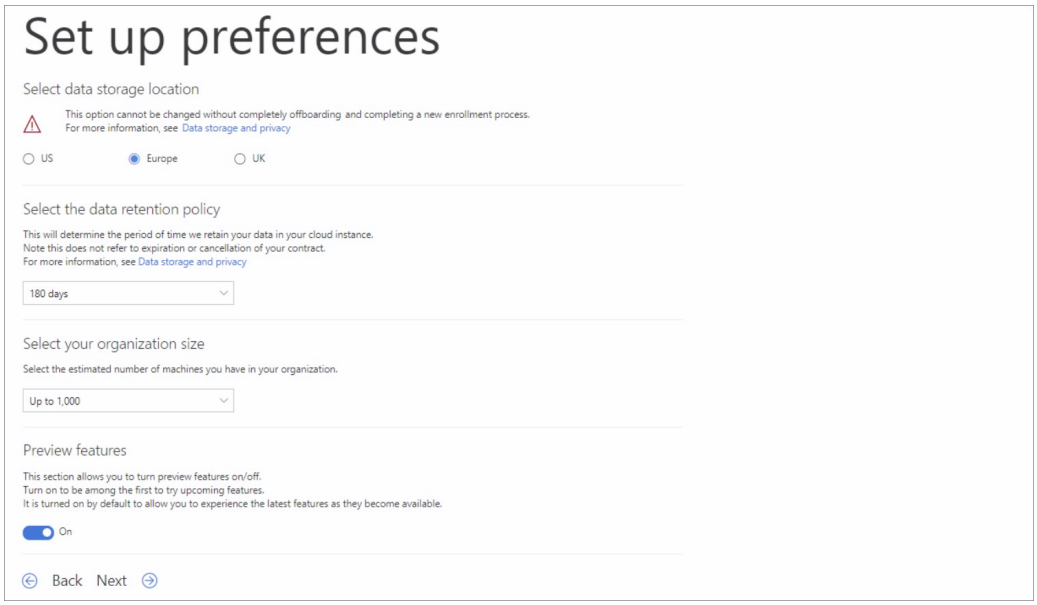


4. Définissez les préférences.

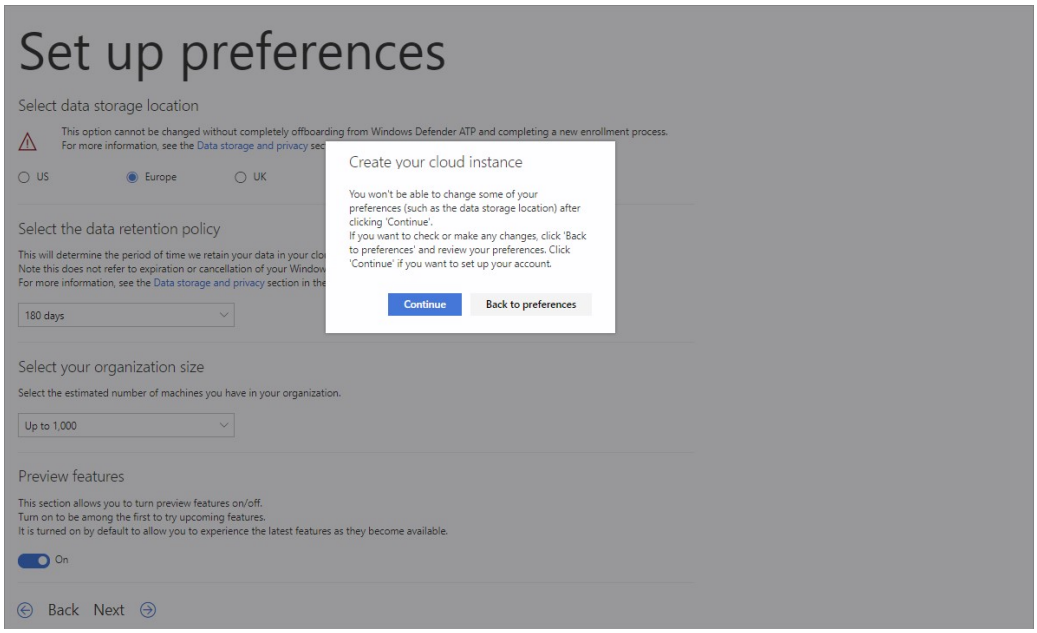
   Emplacement de stockage des données : il est important de le configurer correctement. Déterminez le lieu d'hébergement principal du client: États-Unis, Europe ou Royaume-Uni. Vous ne pouvez pas modifier l'emplacement après cette configuration et Microsoft ne transférera pas les données à partir de la géolocalisation spécifiée.

   Rétention des données -la valeur par défaut est 6 mois.

   Activer les fonctionnalités d'aperçu -la valeur par défaut est activée et peut être modifiée ultérieurement.



5. Sélectionnez **Suivant**.



6. Sélectionnez **Continuer**.

Configuration du réseau

Si l'organisation n'a pas besoin que les points de terminaison utilisent un proxy pour accéder à Internet, ignorez cette section.

Le capteur Microsoft Defender ATP nécessite Microsoft Windows HTTP (WinHTTP) pour signaler les données du capteur et communiquer avec le service Microsoft Defender ATP. Le capteur Microsoft Defender ATP intégré s'exécute dans le contexte du système à l'aide du compte LocalSystem. Le

capteur utilise les services Microsoft Windows HTTP (WinHTTP) pour permettre une communication avec le service Cloud Microsoft Defender ATP. Le paramètre de configuration WinHTTP est indépendant des paramètres de proxy de navigation Internet de Windows Internet (WinINet), et peut uniquement découvrir un serveur proxy à l'aide des méthodes de découverte suivantes:

Méthodes de découverte automatique:

- Proxy transparent
- Protocole WPAD (Web Proxy Auto-Discovery)

Si un proxy transparent ou WPAD a été implémenté dans la topologie du réseau, il n'est pas nécessaire de configurer des paramètres de configuration particuliers. Pour plus d'informations sur les exclusions d'URL Microsoft Defender ATP dans le proxy, consultez l'annexe de ce document pour connaître les URL de création de listes ou sur les documents Microsoft.

Configuration manuelle de proxy statique:

- Configuration basée sur le registre
- WinHTTP configuré à l'aide de la commande netsh
  Approprié uniquement pour les ordinateurs de bureau d'une topologie stable (par exemple, un bureau dans un réseau d'entreprise derrière le même proxy);

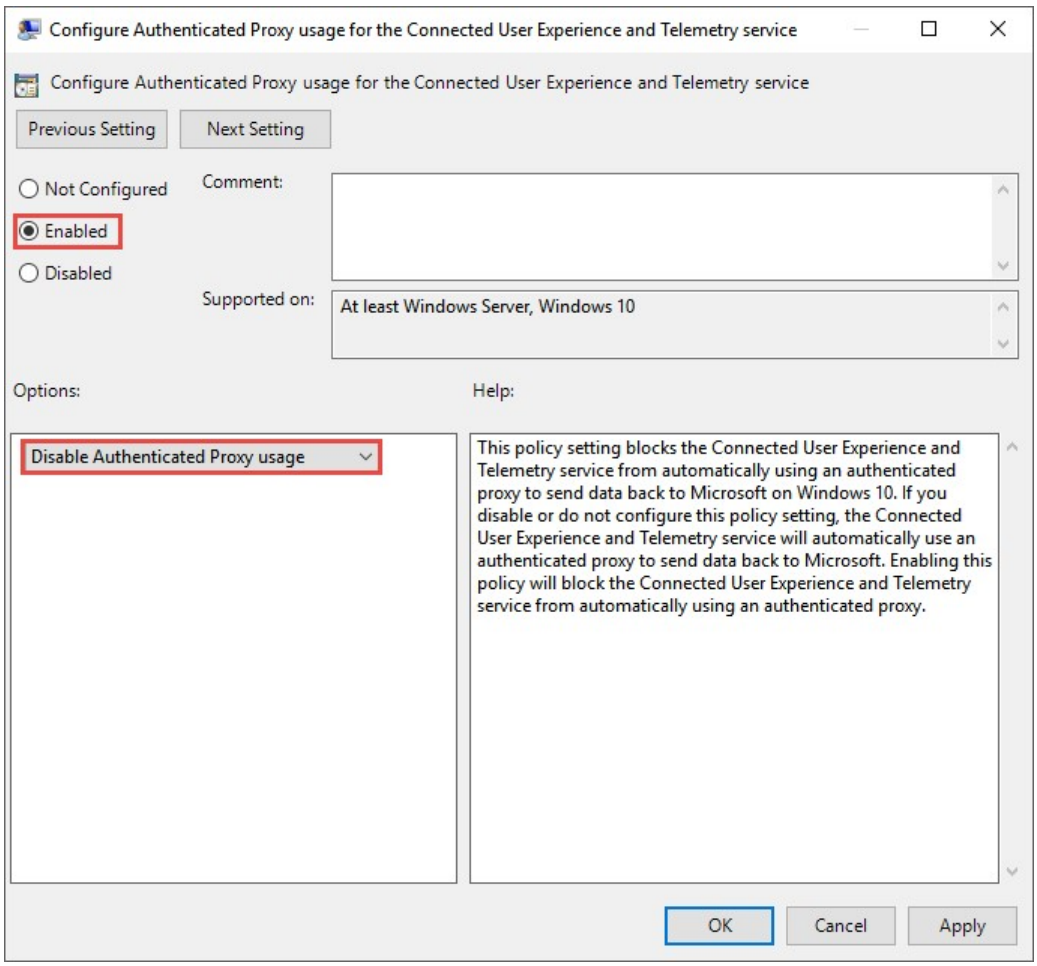
Configurer le serveur proxy manuellement à l'aide d'un proxy statique basé sur registre

Configurer un proxy statique basé sur le registre pour autoriser uniquement le capteur Microsoft Defender ATP à signaler des données de diagnostic et communiquer avec les services ATP de Microsoft Defender si un ordinateur n'est pas autorisé à se connecter à Internet. Le proxy statique est configurable par le biais de la stratégie de groupe. La stratégie de groupe se trouve sous:

- Modèles d'administration \ > composants Windows \ > la collection de données et les versions d'évaluation \ > configurer l'utilisation du proxy authentifié pour le service d'expérimentation et de télémétrie des utilisateurs connectés

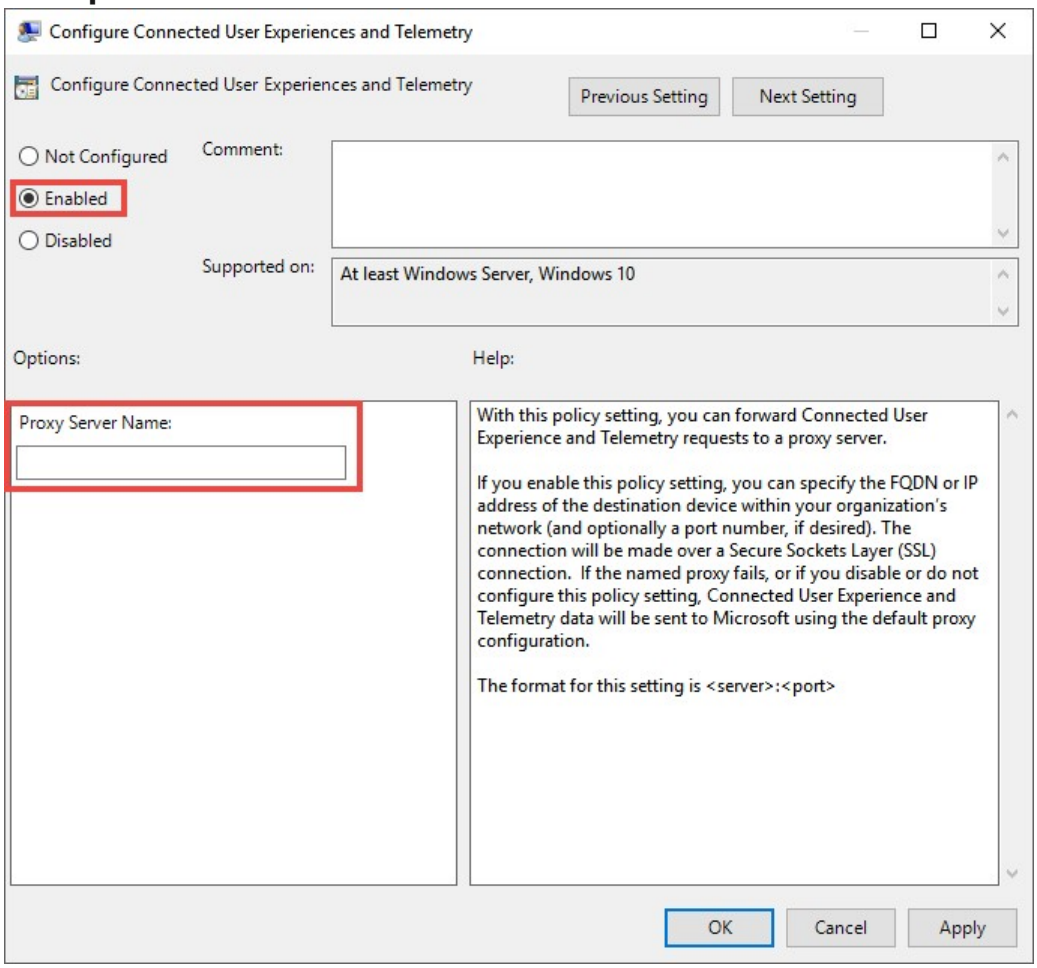
- Activez l' **option activée** et sélectionnez **désactiver l'utilisation du proxy authentifié** .

1. Ouvrez la console de gestion des stratégies de groupe.
2. Création d'une stratégie ou modification d'une stratégie existante basée sur les pratiques de l'organisation.
3. Modifiez la stratégie de groupe et naviguez jusqu'à **modèles d'administration \ > composants Windows \ > la collection de données et les versions d'évaluation \ > configurer l'utilisation du proxy authentifié pour le service d'expérimentation et de télémétrie de l'utilisateur connecté**.



4. Sélectionnez **Activé**.
5. Sélectionnez **désactiver l'utilisation du proxy authentifié**.
6. Naviguez jusqu'à **modèles d'administration \ > composants Windows \ > collection de données et les versions d'évaluation \ > configurer**

les expériences des utilisateurs connectés et la télémétrie.



7. Sélectionnez **Activé**.

8. Entrez le **nom du serveur proxy**.

La stratégie définit deux valeurs de Registre, `TelemetryProxyServer` comme REG_SZ et `DisableEnterpriseAuthProxy` comme REG_DWORD sous la clé de Registre `HKLM\Software\Policies\Microsoft\Windows\DataCollection`.

La valeur de Registre `TelemetryProxyServer` prend le format de chaîne suivant:

text	Copier
`<server name or ip>:<port>`	

Par exemple: 10.0.0.6:8080

La valeur de Registre `DisableEnterpriseAuthProxy` doit être réglée sur1.

Configurer le serveur proxy manuellement à l'aide de la commande netsh

Utilisez netsh pour configurer un proxy statique à l'échelle du système.

> ⓘ **Notes**
>
> - Cela affecte toutes les applications, notamment les servicesWindows qui utilisent WinHTTP avec le proxy par défaut.
> - Les ordinateurs portables qui changent de topologie (par exemple: du bureau au domicile) ne fonctionneront pas correctement avec netsh. Utilisez la configuration de proxy statique basé sur le Registre.

1. Ouvrez une ligne de commande avec élévation de privilèges:

   a. Accédez à **Démarrer** et tapez **cmd**.

   b. Cliquez avec le bouton droit sur **Invite de commandes**, puis sélectionnez **Exécuter en tant qu'administrateur**.

2. Entrez la commande suivante et appuyez sur **Entrée**:

PowerShell	Copier
`netsh winhttp set proxy <proxy>:<port>`	

   Par exemple: netsh winhttp définit le proxy 10.0.0.6:8080

Configuration du proxy pour les machines de niveau inférieur

Les machines de niveau inférieur incluent les stations de travail Windows 7 SP1 et Windows 8,1 ainsi que Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 et les versions de Windows Server 2016 antérieures à Windows Server CB 1803. Ces systèmes d'exploitation disposent du proxy configuré dans le cadre de l'agent de gestion Microsoft pour gérer la communication entre le point de terminaison et Azure. Pour plus d'informations sur la configuration d'un proxy sur ces ordinateurs, voir le Guide de déploiement rapide de Microsoft Management Agent.

URL du service proxy

Les URL qui incluent v20 dans ces derniers sont nécessaires uniquement si vous disposez de Windows 10 version 1803 ou ultérieure. Par exemple, `us-v20.events.data.microsoft.com` n'est nécessaire que si l'ordinateur est équipé de Windows 10, version 1803 ou ultérieure.

Emplacement du service	Enregistrement DNS Microsoft.com

URL courantes de tous les emplacements	`crl.microsoft.com`
	`ctldl.windowsupdate.com`
	`events.data.microsoft.com`
	`notify.windows.com`
	`settings-win.data.microsoft.com`

Union européenne	`eu.vortex-win.data.microsoft.com`
	`eu-v20.events.data.microsoft.com`
	`usseu1northprod.blob.core.windows.net`
	`usseu1westprod.blob.core.windows.net`
	`winatp-gw-neu.microsoft.com`
	`winatp-gw-weu.microsoft.com`
	`wseu1northprod.blob.core.windows.net`
	`wseu1westprod.blob.core.windows.net`

Royaume-Uni	`uk.vortex-win.data.microsoft.com`
	`uk-v20.events.data.microsoft.com`
	`ussuk1southprod.blob.core.windows.net`
	`ussuk1westprod.blob.core.windows.net`
	`winatp-gw-uks.microsoft.com`
	`winatp-gw-ukw.microsoft.com`
	`wsuk1southprod.blob.core.windows.net`
	`wsuk1westprod.blob.core.windows.net`

États-Unis	`us.vortex-win.data.microsoft.com`
	`ussus1eastprod.blob.core.windows.net`
	`ussus1westprod.blob.core.windows.net`
	`ussus2eastprod.blob.core.windows.net`
	`ussus2westprod.blob.core.windows.net`
	`ussus3eastprod.blob.core.windows.net`
	`ussus3westprod.blob.core.windows.net`
	`ussus4eastprod.blob.core.windows.net`
	`ussus4westprod.blob.core.windows.net`
	`us-v20.events.data.microsoft.com`
	`winatp-gw-cus.microsoft.com`

Emplacement du service	Enregistrement DNS Microsoft.com
	winatp-gw-eus.microsoft.com wsus1eastprod.blob.core.windows.net wsus1westprod.blob.core.windows.net wsus2eastprod.blob.core.windows.net wsus2westprod.blob.core.windows.net

Si un proxy ou un pare-feu bloque le trafic anonyme, lorsque le capteur Microsoft Defender ATP est connecté à partir du contexte du système, assurez-vous que le trafic anonyme est autorisé dans les URL précédemment répertoriées.

Plage d'adresses IP principales du service Microsoft Defender ATP

Si vous avez des périphériques réseau qui ne prennent pas en charge les URL blanches mentionnées dans la section précédente, vous pouvez utiliser les informations suivantes.

Microsoft Defender ATP est bâti sur Azure Cloud et déployé dans les régions suivantes:

- \ + \ <nom de la région = «uswestcentral» >
- \ + \ <nom de la région = «useast2» >
- \ + \ <nom de la région = «USEast» >
- \ + \ <nom de la région = «europenorth» >
- \ + \ <nom de la région = «EuropeWest» >
- \ + \ <nom de la région = «uksouth» >
- \ + \ <nom de la région = «ukwest» >

Vous pouvez trouver la plage d'adresses IP Azure dans les plages d'adresses IP de Microsoft Azure Datacenter.

> ⓘ **Notes**
>
> Dans le cadre d'une solution basée sur le Cloud, la plage d'adresses IP peut changer. Nous vous recommandons de basculer vers le paramètre de résolution DNS.

Étape suivante

 Étape 3: intégration	Appareils intégrés au service, afin que le service ATP de Microsoft Defender puisse y obtenir des données de capteur

Cette page est-elle utile ?

Yes No