

Configurer le déploiement de Microsoft Defender ATP

03/04/2020 • 6 minutes de lecture •  

Dans cet article

[Vérifier l'état de la licence](#)

[Validation du fournisseur de services cloud](#)

[Configuration du client](#)

[Configuration du réseau](#)

[Étape suivante](#)

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

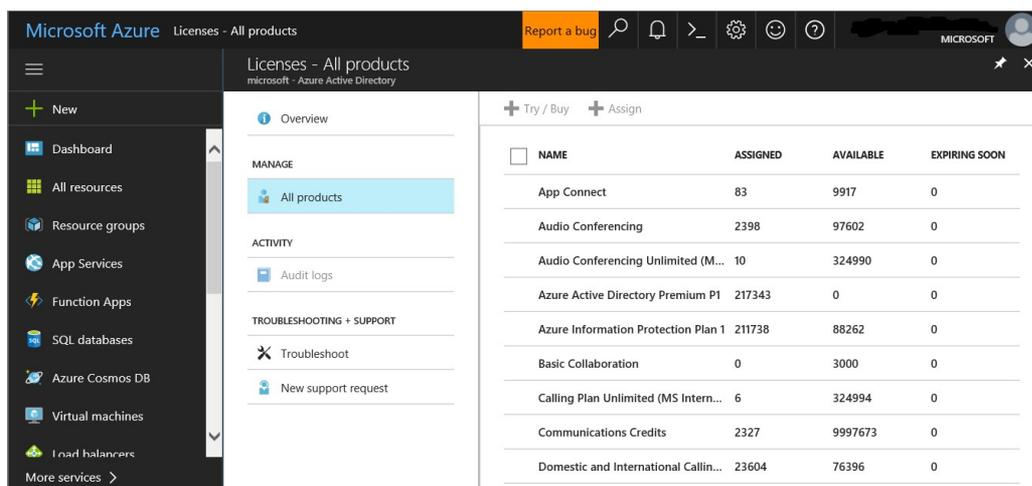
Pour vous guider dans le cadre d'un déploiement standard, ce scénario traite uniquement de l'utilisation du gestionnaire de configuration de point de terminaison Microsoft. Microsoft Defender ATP prend en charge l'utilisation d'autres outils d'intégration, mais ne sera pas couvert par ces

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 effectués par le biais du centre d'administration ou du **portail Microsoft Azure**.

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



NAME	ASSIGNED	AVAILABLE	EXPIRING SOON
App Connect	83	9917	0
Audio Conferencing	2398	97602	0
Audio Conferencing Unlimited (M...	10	324990	0
Azure Active Directory Premium P1	217343	0	0
Azure Information Protection Plan 1	211738	88262	0
Basic Collaboration	0	3000	0
Calling Plan Unlimited (MS Intern...	6	324994	0
Communications Credits	2327	9997673	0
Domestic and International Callin...	23604	76396	0

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.

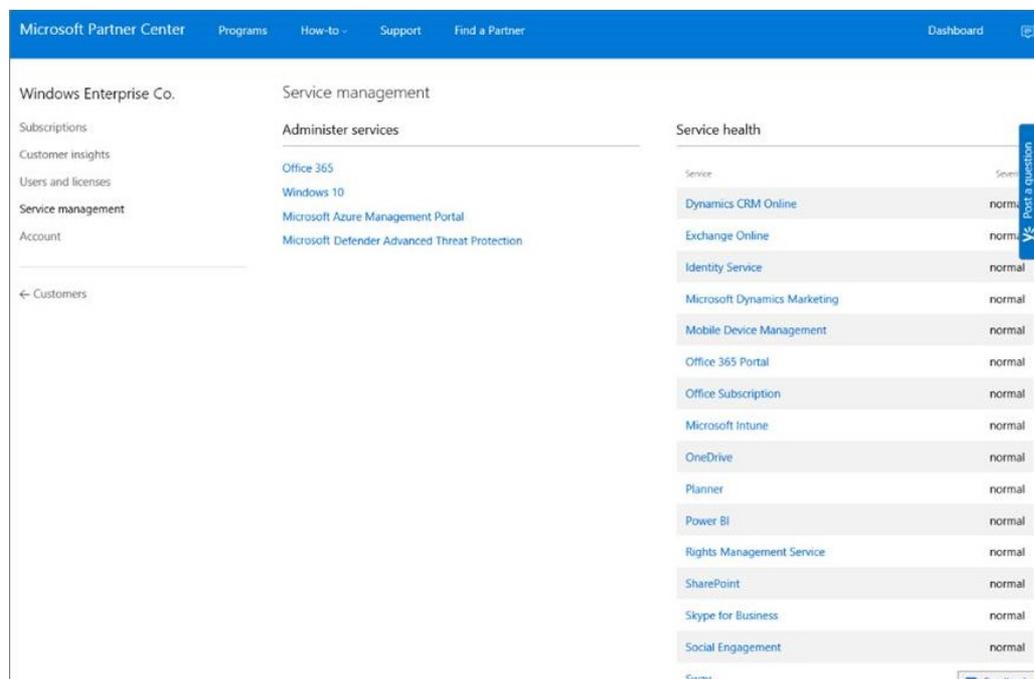


Licenses	
Available	1000000
Assigned ⓘ	0
Assign to users	

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.com> accédez à.

Dear Admin

This wizard will guide you through the steps to onboard your organization.

You need to be a global administrator or security administrator in your [Azure Active Directory](#) to complete this wizard. For more information on how to setup the required user permissions, see [Assign user access to the portal](#).

Click Refresh when you've completed assigning user access roles.

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\(\)](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.

Welcome SecAdmin

This wizard will guide you through the steps to onboard your organization.

For more detailed help and information on the onboarding process, see [Onboard machines and set up access](#).

For more information about how Windows Defender ATP stores and retains your data, see [Data storage and privacy](#).

You need to set aside 10 to 20 minutes to complete the process, although it might take longer before all onboarded machines appear in the portal.

Click 'Next' to start the onboarding process.

⏪ Back Next ⏩

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.

Set up preferences

Select data storage location

This option cannot be changed without completely offboarding and completing a new enrollment process.
For more information, see [Data storage and privacy](#)

US Europe UK

Select the data retention policy

This will determine the period of time we retain your data in your cloud instance.
Note this does not refer to expiration or cancellation of your contract.
For more information, see [Data storage and privacy](#)

180 days

Select your organization size

Select the estimated number of machines you have in your organization.

Up to 1,000

Preview features

This section allows you to turn preview features on/off.
Turn on to be among the first to try upcoming features.
It is turned on by default to allow you to experience the latest features as they become available.

On

[← Back](#) [Next →](#)

5. Sélectionnez **Suivant**.

Set up preferences

Select data storage location

This option cannot be changed without completely offboarding from Windows Defender ATP and completing a new enrollment process.
For more information, see the [Data storage and privacy](#) section in the Windows Defender ATP documentation.

US Europe UK

Select the data retention policy

This will determine the period of time we retain your data in your cloud instance.
Note this does not refer to expiration or cancellation of your Windows Defender ATP account.
For more information, see the [Data storage and privacy](#) section in the Windows Defender ATP documentation.

180 days

Select your organization size

Select the estimated number of machines you have in your organization.

Up to 1,000

Preview features

This section allows you to turn preview features on/off.
Turn on to be among the first to try upcoming features.
It is turned on by default to allow you to experience the latest features as they become available.

On

[← Back](#) [Next →](#)

Create your cloud instance

You won't be able to change some of your preferences (such as the data storage location) after clicking 'Continue'.

If you want to check or make any changes, click 'Back to preferences' and review your preferences. Click 'Continue' if you want to set up your account.

[Continue](#) [Back to preferences](#)

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);

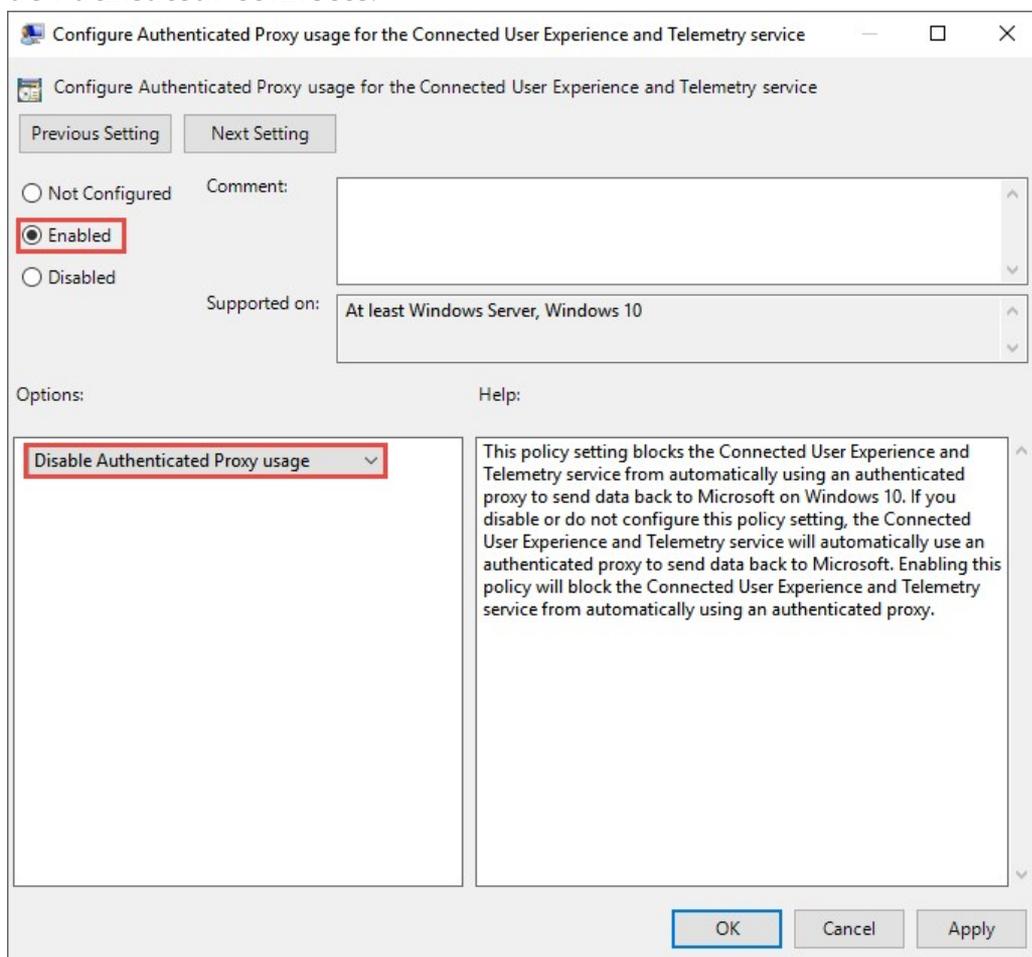
Configurer le serveur proxy manuellement à l'aide d'un proxy statique basé sur registre

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.

Configure Connected User Experiences and Telemetry

Configure Connected User Experiences and Telemetry Previous Setting Next Setting

Not Configured Comment:

Enabled

Disabled Supported on: At least Windows Server, Windows 10

Options: Proxy Server Name:

Help: With this policy setting, you can forward Connected User Experience and Telemetry requests to a proxy server. If you enable this policy setting, you can specify the FQDN or IP address of the destination device within your organization's network (and optionally a port number, if desired). The connection will be made over a Secure Sockets Layer (SSL) connection. If the named proxy fails, or if you disable or do not configure this policy setting, Connected User Experience and Telemetry data will be sent to Microsoft using the default proxy configuration. The format for this setting is <server>:<port>

OK Cancel Apply

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 sur 1.

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 services Windows 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
<pre>netsh winhttp set proxy <proxy>:<port></pre>	

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	<code>cr1.microsoft.com</code> <code>ctldl.windowsupdate.com</code> <code>events.data.microsoft.com</code> <code>notify.windows.com</code> <code>settings-win.data.microsoft.com</code>
Union européenne	<code>eu.vortex-win.data.microsoft.com</code> <code>eu-v20.events.data.microsoft.com</code> <code>usseu1northprod.blob.core.windows.net</code> <code>usseu1westprod.blob.core.windows.net</code> <code>winatp-gw-neu.microsoft.com</code> <code>winatp-gw-weu.microsoft.com</code> <code>wseu1northprod.blob.core.windows.net</code> <code>wseu1westprod.blob.core.windows.net</code>
Royaume-Uni	<code>uk.vortex-win.data.microsoft.com</code> <code>uk-v20.events.data.microsoft.com</code> <code>ussuk1southprod.blob.core.windows.net</code> <code>ussuk1westprod.blob.core.windows.net</code> <code>winatp-gw-uks.microsoft.com</code> <code>winatp-gw-ukw.microsoft.com</code> <code>wsuk1southprod.blob.core.windows.net</code> <code>wsuk1westprod.blob.core.windows.net</code>
États-Unis	<code>us.vortex-win.data.microsoft.com</code> <code>ussus1eastprod.blob.core.windows.net</code> <code>ussus1westprod.blob.core.windows.net</code> <code>ussus2eastprod.blob.core.windows.net</code> <code>ussus2westprod.blob.core.windows.net</code> <code>ussus3eastprod.blob.core.windows.net</code> <code>ussus3westprod.blob.core.windows.net</code> <code>ussus4eastprod.blob.core.windows.net</code> <code>ussus4westprod.blob.core.windows.net</code> <code>us-v20.events.data.microsoft.com</code> <code>winatp-gw-cus.microsoft.com</code>

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
