

# Meilleures pratiques pour les utilisateurs Cisco Umbrella

## Table des matières

---

[Introduction](#)

[État du système et état du service Cisco Umbrella](#)

[Enregistrement du réseau](#)

[Pare-feu et proxys locaux](#)

[La phase de déploiement](#)

[Page Proxy intelligent / Bloquer](#)

[Appareils virtuels Cisco Umbrella](#)

[Intégrations de tiers](#)

[Intégration Active Directory](#)

[Clients itinérants](#)

[Journalisation](#)

[Meilleures pratiques de la console de services gérés](#)

[Authentification à deux facteurs](#)

[Contacter et travailler avec l'équipe d'assistance Cisco Umbrella](#)

---

## Introduction

Ce document décrit les différentes meilleures pratiques relatives à Cisco Umbrella.

## État du système et état du service Cisco Umbrella

- Ajoutez les signets <http://208.69.38.170/> et <https://146.112.59.2/#/> afin de pouvoir vérifier les pages d'état du système Umbrella même si le DNS local n'est pas disponible.
- Abonnez-vous à la page d'état du service Cisco Umbrella à l'adresse <https://146.112.59.2/#/> pour recevoir des notifications sur les dégradations de service, les interruptions de service et/ou la maintenance et les événements.
- Suivez les pages Service Updates and Announcements de la base de connaissances Cisco Umbrella.
- Consultez régulièrement le tableau de bord Cisco Umbrella « Message Center » pour obtenir des alertes et des notifications sur les produits.

## Enregistrement du réseau

Toutes les adresses IP et les plages CIDR d'adresses IP associées à votre entreprise doivent être enregistrées auprès d'Umbrella. Pour plus d'informations, consultez [la documentation d'Umbrella](#).

## Pare-feu et proxies locaux

- Configurez les pare-feu locaux pour autoriser les plages CIDR d'adresses IP Umbrella.
- Si vous utilisez un proxy HTTP, assurez-vous qu'il est configuré.

## La phase de déploiement

- Si possible, déployez-les progressivement et testez-les avant de les déployer en masse. Pour tester de nouvelles fonctionnalités, appliquez une stratégie à un sous-ensemble d'utilisateurs et d'ordinateurs. Si le test réussit, appliquez la stratégie à davantage d'utilisateurs et d'ordinateurs.
- Utilisez le Testeur de stratégies pour vérifier la fonctionnalité de stratégie prévue pour les identités et les domaines individuels.
- Vérifiez le fonctionnement en visitant les pages de test avec un navigateur. Pour plus d'informations, consultez : Comment : Testez avec succès pour vous assurer que vous exécutez Umbrella correctement.
- Créez un ou plusieurs rapports planifiés pour surveiller votre environnement et détecter les événements liés à la sécurité. Pour plus d'informations à ce sujet, consultez la [documentation Umbrella](#).

## Page Proxy intelligent / Bloquer

- Incluez l'[autorité de certification racine](#) dans votre déploiement, en particulier si vous utilisez ou prévoyez d'utiliser les fonctionnalités du proxy intelligent. C'est aussi une bonne idée de l'installer quand même, comme les sites bloqués quand ils sont https:// (ex : <https://facebook.com>) génèrent des erreurs sans elle.

## Appareils virtuels Cisco Umbrella

- Si vous utilisez des appliances virtuelles (VA), assurez-vous que la liste [Domaines internes](#) est remplie avant le déploiement.
- Si vous utilisez des appliances virtuelles sur VMWare, utilisez des adaptateurs VMXNET3 conformément à la .
- Si vous utilisez des appliances virtuelles, vérifiez régulièrement la console de chaque appliance virtuelle via l'hôte VMWare ou Hyper-V. Sur le côté droit, toutes les entrées Services et Connectivité s'affichent en vert.
- Configurez les serveurs DNS internes comme indiqué ici : Quelle est la configuration recommandée pour les serveurs DNS internes lors du déploiement d'Umbrella ?

## Intégrations de tiers

- Si vous utilisez des intégrations telles que Check Point ou Cisco AMP Threat Grid, ajoutez tous les domaines que vous souhaitez ne jamais avoir bloqués à la liste verte globale (ou à d'autres listes de domaines conformément à vos politiques générales) :

- La page d'accueil de votre entreprise (mydomain.com).
- Domaines représentant des services que vous fournissez et pouvant avoir des enregistrements internes et externes (mail.my servicedomain.com, portal.myotherservicedomain.com).
- Il peut y avoir des applications cloud moins connues dont vous dépendez fortement et que Cisco Umbrella connaît ou n'inclut pas dans leur validation automatique de domaine (localcloudservice.com)

## Intégration Active Directory

- Si Cisco Umbrella est intégré à Active Directory, ajoutez des comptes de service à la [liste Exceptions utilisateur AD](#).

## Clients itinérants

- Si vous utilisez des clients itinérants, assurez-vous que la [liste Domaines internes](#) est remplie.
- Assurez-vous que tous vos clients itinérants sont sur la même version sur le tableau de bord Cisco Umbrella à Identities > Roaming Computers.
- Si vous utilisez Cisco Secure Client (anciennement AnyConnect), utilisez le module de sécurité d'itinérance Umbrella au lieu du client d'itinérance autonome.
- Si vous utilisez un client d'itinérance sur un réseau Wi-Fi de compagnie aérienne, reportez-vous aux Méthodes Recommandées pour les clients d'itinérance et les réseaux Wi-Fi de compagnie aérienne/hôtel.

## Journalisation

Les journaux détaillés ne sont conservés que pendant 30 jours, puis ils sont décomposés en données de rapport agrégées. Si vous souhaitez conserver une copie des données plus détaillées plus longtemps que 30 jours, configurez un compartiment Amazon S3 pour exporter vos données dans Paramètres > Gestion des journaux.

## Meilleures pratiques de la console de services gérés

Intégration de MSP Professional Services Automation (PSA) de la console de services gérés :

- Si vous êtes un [MSP intégré à un PSA](#), vérifiez que l'icône « PSA INTEGRATION » s'affiche en vert.

## Authentification à deux facteurs

- [Implémentez l'authentification à deux facteurs](#) pour les utilisateurs Cisco Umbrella.
- Mettez en oeuvre une authentification en deux étapes pour les administrateurs Cisco Umbrella MSP.

## Contacter et travailler avec l'équipe d'assistance Cisco Umbrella

- Après vous être connecté au tableau de bord Umbrella, envoyez une demande à l'équipe d'assistance Umbrella via le formulaire Web sur la page de demande.
- Si vous avez souscrit une assistance téléphonique auprès de Cisco Umbrella, une icône représentant un téléphone s'affiche dans l'angle supérieur droit du tableau de bord Cisco Umbrella. Cliquez sur l'icône représentant un téléphone pour afficher le numéro de téléphone de l'assistance.
- Fournissez des détails complets sur vos problèmes ou questions.
- Utilisez le résultat de l'outil de diagnostic Umbrella pour votre dossier d'assistance.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.