



## **Guide des agents des services de terminaux (TS) Cisco, version 1.2**

**Dernière modification :** 2025-06-06

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2018 Cisco Systems, Inc. Tous droits réservés.



## TABLE DES MATIÈRES

---

### CHAPITRE 1

#### **Introduction à l'agent de services de terminaux de Management Center 1**

- À propos de l'Agent Terminal Services (TS) 1
- Exigences en matière d'environnement de serveur et de système 2
- Résolution des problèmes du Firepower Management Center avec l'Agent TS 3
- Dépanner le problème en utilisant l'Agent TS 6
- Dépanner le problème en utilisant l'Agent utilisateur 7
- Problèmes connus et problèmes résolus 8
- Historique pour l'Agent TS 9

---

### CHAPITRE 2

#### **Installer et configurer l'ASA de l'Agent TS 11**

- Installer ou mettre à niveau l'Agent TS 11
- Démarrer l'interface de configuration de l'Agent TS 12
- Configurer l'Agent TS 12
  - Champs de configuration de l'Agent TS 13
- Création du rôle VDI REST 19

---

### CHAPITRE 3

#### **Afficher les données de l'Agent TS 21**

- Afficher les informations sur l'Agent TS 21
- Afficher l'état de la connexion 22
- Afficher les données de l'utilisateur, de la session utilisateur et de connexion TCP/UDP de l'Agent TS sur le FMC 23

---

### CHAPITRE 4

#### **Gérer l'Agent TS 25**

- Mettre fin à une session d'utilisateur en cours 25
- Affichage de l'état du composant du service de l'Agent TS 25
- Démarrage et arrêt des processus de l'Agent TS 26

Affichage des journaux d'activité de l'Agent TS sur le serveur 26

Désinstallation de l'Agent TS 26



# CHAPITRE 1

## Introduction à l'agent de services de terminaux de Management Center

---

- À propos de l'Agent Terminal Services (TS), à la page 1
- Exigences en matière d'environnement de serveur et de système, à la page 2
- Résolution des problèmes du Firepower Management Center avec l'Agent TS, à la page 3
- Dépanner le problème en utilisant l'Agent TS, à la page 6
- Dépanner le problème en utilisant l'Agent utilisateur, à la page 7
- Problèmes connus et problèmes résolus, à la page 8
- Historique pour l'Agent TS, à la page 9

### À propos de l'Agent Terminal Services (TS)

L'agent de services de terminaux Cisco permet à Cisco Firepower Management Center d'identifier de façon unique le trafic utilisateur surveillé par un serveur de terminaux Microsoft Windows. Sans le Agent TS, les systèmes reconnaissent tout le trafic provenant d'un serveur de terminaux Microsoft Windows comme une seule session utilisateur provenant d'une adresse IP.



---

**Remarque** Pour éviter les problèmes potentiels et pour vous assurer que vous utilisez le logiciel le plus récent, Cisco vous recommande d'utiliser la dernière version publiée de Agent TS. Pour trouver la dernière version, accédez au [site d'assistance Cisco](#).

---

Lorsqu'il est installé et configuré sur votre serveur de terminaux Microsoft Windows, le Agent TS attribue une plage de ports aux sessions utilisateur individuelles et les ports de cette plage aux connexions TCP et UDP dans la session utilisateur. Les systèmes utilisent des ports uniques pour identifier les connexions TCP et UDP individuelles par les utilisateurs sur le réseau. Les plages de ports sont attribuées selon le principe du moins récemment utilisé, ce qui signifie qu'après la fin d'une session utilisateur, la même plage de ports n'est pas immédiatement réutilisée pour les nouvelles sessions utilisateur.



---

**Remarque** Les messages ICMP sont transmis sans mappage de port.

---

Le trafic généré par un service exécuté dans le contexte système de l'ordinateur n'est pas suivi par le Agent TS. En particulier, le Agent TS n'identifie pas le trafic de blocage de message du serveur (SMB), car le trafic SMB est exécuté dans le contexte système.

Le Agent TS prend en charge jusqu'à 199 sessions utilisateur simultanées par hôte Agent TS. Si un seul utilisateur exécute plusieurs sessions utilisateur simultanées, le Agent TS attribue une plage de ports unique à chaque session utilisateur individuelle. Lorsqu'un utilisateur met fin à une session, le Agent TS peut utiliser cette plage de ports pour une autre session utilisateur.

Chaque FMC prend en charge jusqu'à 50 Agent TS, qui s'y connectent en même temps.

Trois composants principaux de Agent TS sont installés sur votre serveur :

- Interface : application pour configurer le Agent TS et surveiller les sessions utilisateur actuelles
- Service : programme qui surveille les connexions et les déconnexions des utilisateurs.
- Pilote – programme qui effectue la traduction de port

Le Agent TS peut être utilisé pour éléments suivants :

- Les données Agent TS sur le FMC peuvent être utilisées pour la sensibilisation et le contrôle de l'utilisateur. Pour en savoir plus sur l'utilisation des données Agent TS du système, consultez le *Guide de configuration de Cisco Secure Firewall Management Center*.




---

**Remarque**

Pour utiliser Agent TS à des fins de sensibilisation et de contrôle des utilisateurs, vous devez le configurer pour envoyer des données *uniquement* à FMC. Pour en savoir plus, consultez [Configure the Agent TS](#) (configurer le).

---

## Exigences en matière d'environnement de serveur et de système

Vous devez satisfaire aux exigences suivantes pour installer et exécuter le Agent TS sur votre système.




---

**Remarque**

Pour éviter les problèmes potentiels et pour vous assurer que vous utilisez le logiciel le plus récent, Cisco vous recommande d'utiliser la dernière version publiée de Agent TS. Pour trouver la dernière version, accédez au [site d'assistance Cisco](#).

---

### Exigences en termes de serveur

Installez-le Agent TS sur l'une des versions de serveur de terminaux Microsoft Windows de 64 bits suivantes :

- Microsoft Windows Server 2016
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Windows Server 2012 R de Microsoft 2



---

**Remarque** L'installation Agent TS nécessite 653 Ko d'espace libre sur votre serveur.

---



---

**Remarque** Si le serveur Agent TS utilise un logiciel antivirus qui traite le trafic Web, le trafic utilisateur est généralement affecté à l'utilisateur système et le FMC voit ces utilisateurs comme Inconnu. Pour éviter le problème, désactivez la fonction de mandataire pour le trafic Web.

---

Le Agent TS est compatible avec l'une des solutions de services de terminaux suivantes installées sur votre serveur :

- Citrix XenDesktop
- Citrix XenApp
- Hyperviseur de projet Xen
- Hyperviseur VMware vSphere/VMware ESXi 6.0
- Services de terminaux Windows/Services de bureau à distance Windows (RDS)

Cette version de l'Agent TS prend en charge l'utilisation d'un contrôleur d'interface réseau (NIC) unique pour la traduction de ports et les communications entre systèmes de serveurs. Si au moins deux cartes réseau valides sont présentes sur votre serveur, l'Agent TS effectue la traduction de port uniquement sur l'adresse que vous précisez lors de la configuration. Une carte réseau valide doit avoir une adresse IPv4 ou IPv6 unique, ou une de chaque type; une carte réseau valide ne peut pas avoir plusieurs adresses du même type.



---

**Remarque** Si les annonces de routeur sont activées sur des appareils connectés à votre serveur, les appareils peuvent attribuer plusieurs adresses IPv6 aux NIC sur votre serveur et invalider les NIC pour une utilisation avec Agent TS.

---

#### **Configuration système requise**

Cette version des Agent TS prend en charge la connexion aux FMC autonomes ou à haute disponibilité exécutant la version 6.2 ou une version ultérieure du Système.

## **Résolution des problèmes du Firepower Management Center avec l'Agent TS**

Consultez les sections suivantes pour plus de renseignements sur le dépannage des problèmes du Firepower Management Center avec l'agent TS.

Pour en savoir plus sur les problèmes connus et résolus de cette version, consultez [Problèmes connus et problèmes résolus](#), à la page 8.

### FMC n'affiche pas les renseignements sur les utilisateurs pour les processus du système

Le trafic généré par un service s'exécutant dans le contexte système n'est pas suivi par le Agent TS. Notez en particulier les éléments suivants :

- Le Agent TS n'identifie pas le trafic de blocage de message du serveur (SMB), car le trafic SMB s'exécute dans le contexte système.
- Certaines applications d'antivirus transmettent le trafic Web à une passerelle locale ou en nuage pour intercepter les virus avant qu'ils n'atteignent un ordinateur client. Cependant, cela signifie que le logiciel antivirus utilise généralement le compte système; dans ce cas, le FMC voit les utilisateurs comme inconnus. Pour résoudre le problème, désactivez le proxy du trafic Web.

### les délais d'attente des utilisateurs Agent TS ne sont pas respectés

Vous devez synchroniser l'heure sur votre serveur avec l'heure affichée sur FMC.

### Agent TS ne traduit pas les ports de session des utilisateurs

Le Agent TS n'effectue pas de traduction de port dans les cas suivants :

- Une session d'utilisateur dépasse la valeur **Max User Sessions** (Nombre maximal de sessions d'utilisateur) définie. Par exemple, si la valeur **Max User Sessions** (Nombre maximal de sessions d'utilisateur) est définie sur 29, le Agent TS n'effectue pas de traduction de port sur la 30e session utilisateur.
- Tous les ports disponibles sont utilisés. Par exemple, si votre valeur **User Ports** (Ports utilisateur) **Range** (Plage) désigne 1000 ports par session d'utilisateur, le Agent TS n'effectue pas de traduction de port sur la 1001e TCP/UDP jusqu'à ce que l'utilisateur met fin à une autre connexion TCP/UDP et libère un port.
- Une session d'utilisateur n'a pas de domaine associé. Par exemple, si la session d'un administrateur de serveur est authentifiée par le système local et non par un serveur Active Directory externe, l'administrateur du serveur se connecte au serveur, mais ne peut pas accéder au réseau et le Agent TS n'attribue pas de ports à la session utilisateur.

### Les sessions d'utilisateur ne sont pas rapportées au FMC comme prévu

Si vous mettez à jour la configuration de Agent TS pour vous connecter à un autre FMC, vous devez mettre fin à toutes les sessions utilisateur en cours avant d'enregistrer la nouvelle configuration. Pour en savoir plus, consultez [Mettre fin à une session d'utilisateur en cours, à la page 25](#).

### Le trafic des applications clientes est signalé au FMC comme trafic utilisateur

Si une application cliente est installée sur votre serveur et que l'application est configurée pour se lier à un connecteur qui utilise un port qui ne figure pas dans vos **System Ports** (Ports système), vous devez utiliser le champ **Exclude Port(s)** (Exclure port[s]) pour exclure ce port de la traduction. Si vous n'excluez pas le port et qu'il fait partie de vos **ports utilisateur**, le Agent TS peut signaler le trafic sur ce port comme trafic utilisateur non lié.

Pour éviter cela, configurez votre application client pour se lier à un connecteur qui utilise un port compris dans votre **System Ports** (Ports du système).

### Le délai d'expiration de l'application du serveur, le délai d'expiration du navigateur ou l'échec de connexion de Agent TS-FMC

Si une application sur le serveur Agent TS met fin à une connexion TCP/UDP, mais ferme incomplètement le port associé, le Agent TS ne peut pas utiliser ce port pour la traduction. Si le Agent TS tente d'utiliser le port pour la traduction avant que le serveur ne ferme complètement le port, la connexion échoue.



**Remarque** Vous pouvez utiliser la commande `netstat` (pour un résumé) ou la commande `netstat -a -o -n -b` (pour des renseignements détaillés) pour désigner les ports incomplètement fermés; ces ports ont l'état `TEMP_WAIT` ou `CLOSE_WAIT`.

Si vous voyez ce problème, augmentez la plage de ports Agent TS touchée par le problème :

- Le délai d'expiration de l'application du serveur ou du navigateur se produit si un port fermé de manière incorrecte tombe dans la plage **User Ports** (Ports utilisateur).
- Un échec de la connexion Agent TS-FMC se produit si un port fermé de manière incorrecte tombe dans la plage **System Ports** (Ports du système).

### Agent TS-FMC Échec de connexion

Si Agent TS ne parvient pas à établir de connexion avec FMC lorsque vous cliquez sur le bouton **Test** (Tester) pendant la configuration, vérifiez les éléments suivants :

- Assurez-vous que pas plus de 50 clients Agent TS tentent de se connecter au FMC en même temps.
- Confirmez que le **Username** (Nom d'utilisateur) et le **Password** (Mot de passe) que vous avez fournis sont les bonnes informations d'authentification pour un utilisateur FMC disposant des privilèges REST VDI, comme indiqué dans [Création du rôle VDI REST, à la page 19](#).

Vous pouvez afficher les journaux d'audit sur le FMC pour confirmer que l'authentification de l'utilisateur à partir du Agent TS a réussi.

- Si la connexion au FMC secondaire dans une configuration à haute disponibilité échoue immédiatement après la configuration, voici le comportement attendu. Le Agent TS communique avec le FMC actif en tout temps.

Si le secondaire est le FMC, la connexion au FMC principal échoue.

### Des processus système ou des applications sur le serveur sont défectueux

Si un processus système sur votre serveur utilise un port qui ne se trouve pas dans votre plage **System Ports** (Ports système) ou écoute sur celui-ci, vous devez exclure manuellement ce port à l'aide du champ **Exclude Port(s)** (Exclure port[s]) Reserve Port(s) (Réserver port[s]).

Si une application sur votre serveur utilise ou écoute dans sur votre port Citrix MA Client (2598) ou Windows Terminal Server (3389), confirmez que ces ports sont exclus dans le champ **Exclude Port(s)** (Exclure port[s]).

### FMC affiche les utilisateurs inconnus de Agent TS

Le FMC affiche les utilisateurs inconnus du Agent TS dans les situations suivantes :

- Si le composant du pilote Agent TS tombe en panne de façon inattendue, les sessions utilisateur vues pendant le temps d'arrêt sont enregistrées comme des utilisateurs inconnus sur le FMC.

- Certaines applications d'antivirus transmettent le trafic Web à une passerelle locale ou en nuage pour intercepter les virus avant qu'ils n'atteignent un ordinateur client. Cependant, cela signifie que le logiciel antivirus utilise généralement le compte système; dans ce cas, le FMC voit les utilisateurs comme inconnus. Pour résoudre le problème, désactivez le proxy du trafic Web.
- En cas de défaillance du FMC principal dans une configuration à haute disponibilité, les connexions signalées par l'Agent TS pendant les 10 minutes d'arrêt lors du basculement sont gérées comme suit :
  - Si un utilisateur n'a pas été vu précédemment sur le FMC et que l'Agent TS rapporte les données de session d'utilisateur, les données sont enregistrées comme activité d'utilisateur inconnue sur le FMC.
  - Si l'utilisateur a déjà été vu sur le FMC, les données sont traitées normalement.

Après le temps d'arrêt, les utilisateurs inconnus sont réidentifiés et traités selon les règles de votre politique d'identité.

### Les NIC ne s'affichent pas dans la liste des NIC du serveur

Vous devez désactiver les messages d'annonce du routeur sur tous les appareils connectés à votre serveur. Si les annonces de routeur sont activées, les appareils peuvent attribuer plusieurs adresses IPv6 aux NIC sur votre serveur et invalider les NIC pour une utilisation avec Agent TS.

Une carte réseau valide doit avoir une adresse IPv4 ou IPv6 unique, ou une de chaque type; une carte réseau valide ne peut pas avoir plusieurs adresses du même type.

## Dépanner le problème en utilisant l'Agent TS

### Le test de connexion FMC a échoué

Si vous êtes connecté au serveur de l'Agent TS en tant qu'utilisateur local (par opposition à un utilisateur de domaine), le test de connexion Agent TS échoue avec le test FMC. Cela se produit parce que, par défaut, l'Agent TS ne permet pas aux processus système de communiquer sur le réseau.

Pour contourner le problème, effectuez l'une des opérations suivantes :

- Cochez **Unknown Traffic Communication** (Communication du trafic inconnu) sur la page de l'onglet **Configure** (Configurer) pour autoriser le trafic, comme indiqué dans [Champs de configuration de l'Agent TS](#), à la page 13.
- Connectez-vous à l'ordinateur de l'Agent TS en tant qu'utilisateur de domaine plutôt qu'en tant qu'utilisateur local.

### L'Agent TS signale les utilisateurs comme inconnus et règles non correspondantes

Si des agents de services de terminaux d'autres fournisseurs s'exécutent sur le même serveur que l'agent de services de terminaux Cisco (TS), les numéros de port pour les connexions utilisateur peuvent ne pas être dans la plage de ports utilisateur attribuée. Par conséquent, les utilisateurs peuvent être identifiés comme Unknown (Inconnus) et, par conséquent, les règles d'identité ne correspondent pas pour les utilisateurs.

Pour résoudre ce problème, désactivez ou désinstallez les autres agents des services de terminaux s'exécutant sur le même serveur que l'Agent TS de Cisco.

### Agent TS invite à redémarrer lors de la mise à niveau

Parfois, même si l'adresse IP de la machine ne change pas, Agent TS signale un changement d'adresse IP après la mise à niveau et vous invite à redémarrer le serveur. Cela se produit parce que l'Agent TS détecte une différence entre l'adresse IP et la valeur de la clé de registre suivante :

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TSAgent\{IPv4 | IPv6}
```

Si la valeur de clé est différente de l'adresse IP de l'adaptateur principal configurée, Agent TS signale la modification et vous demande d'enregistrer la configuration et de redémarrer l'ordinateur.

Cela peut se produire, par exemple, si l'ordinateur a été recréé ou restauré à partir d'une sauvegarde et que DHCP attribue une nouvelle adresse IP.

Vous pouvez ignorer l'erreur, mais vous devez quand même redémarrer l'ordinateur après la mise à niveau.

### Exceptions lors de l'enregistrement de l'adresse IP Agent TS

Dans de rares cas, des exceptions s'affichent lorsque vous tentez d'enregistrer la configuration Agent TS avec une adresse IP non valide. Une adresse IP non valide peut être de l'une des options suivantes :

- La même adresse IP qu'un autre appareil sur le réseau.
- Modification de l'adresse IP statique dans Windows lorsque l'application Agent TS est ouverte.

Les exceptions comprennent les éléments suivants :

- `System.argumentsException` : un élément avec la même clé a déjà été ajouté.
- `System.NullReferenceException` : référence d'objet non définie sur une instance d'objet.

**Solution de contournement** : définissez l'adresse IP du serveur Agent TS sur une adresse IP valide, enregistrez la configuration Agent TS et redémarrez le serveur.

## Dépanner le problème en utilisant l'Agent utilisateur

Si vous utilisez à la fois l'Agent TS et l'agent d'utilisateur, vous pouvez éviter les erreurs non critiques dans les journaux en excluant l'adresse IP de l'Agent TS de l'agent d'utilisateur. Si le même utilisateur est détecté par l'Agent TS et l'agent d'utilisateur, les erreurs non critiques sont inscrites dans les journaux.

Pour éviter cela, empêchez l'adresse IP de l'Agent TS d'être enregistrée par l'agent d'utilisateur. Pour en savoir plus, consultez le *Guide de configuration de Firepower User Agent*.

# Problèmes connus et problèmes résolus

## Problèmes connus

Numéro d'identification de la mise en garde	Description
<a href="#">CSCvf63615</a>	Au niveau de journalisation 6, des noms de fonctions incorrects s'affichent dans les journaux.
<a href="#">CSCvf25546</a>	Lorsque les adresses IPv4 et IPv6 sont utilisées sur le serveur d'agent TS, moins de ports de mappage sont disponibles que prévu.
<a href="#">CSCvf25342</a>	Si vos Firepower Management Center sont configurés avec une haute disponibilité et que vous précisez les informations de connexion vers un nom d'hôte plutôt qu'à une adresse IP, l'agent TS ne se connecte jamais au nouveau système actif après le basculement.
<a href="#">CSCvf65188</a>	<p>Dans certains cas, les connexions ne sont pas libérées comme prévu après la déconnexion d'un utilisateur du serveur d'agent TS. Parfois, le protocole TCP permet à une connexion obsolète de se poursuivre plus longtemps que prévu. Ce comportement peut être confirmé par le message suivant dans le journal des événements de Windows :</p> <p>Event 4227: TCP/IP failed to establish an outgoing connection because the selected local endpoint was recently used to connect to the same remote endpoint. (Événement 4227 : TCP/IP n'a pas réussi à établir une connexion sortante, car le terminal local sélectionné a récemment été utilisé pour se connecter au même terminal distant.)</p> <p><b>Solutions :</b></p> <ul style="list-style-type: none"> <li>• Augmentez le nombre de ports de la plage.</li> <li>• Réduisez le temps d'attente de la pile TCP jusqu'à ce que ces connexions soient entièrement libérées : <code>TcpTimedWaitDelay</code>, trouvé à l'emplacement suivant dans le registre Windows : <code>HKEY_LOCAL-MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters</code></li> </ul> <p>Pour en savoir plus, consultez la description de <code>TcpTimedWaitDelay</code> sur <a href="#">MSDN</a>.</p>

## Problèmes résolus

Numéro d'identification de la mise en garde	Description
<a href="#">CSCvg65335</a>	L'agent TS vous informe désormais lorsque l'adresse IP du serveur change, après quoi vous devez enregistrer la modification et redémarrer le serveur.
<a href="#">CSCvg65253</a>	Les liaisons IP des utilisateurs sont maintenant envoyées au centre de gestion Cisco Firepower Management Center. Par conséquent, l'erreur suivante ne s'affiche <i>pas</i> dans le journal de la visionneuse d'événements de l'agent TS et dans la colonne <b>Status</b> (État) de la page de l'onglet <b>Monitor</b> (Surveiller) de l'agent TS : <code>FMC_STATS_TO_BE_CONNECT</code> .

## Historique pour l'Agent TS

Fonctionnalités	Version
<ul style="list-style-type: none"> <li>• Détecte un changement d'adresse IP sur le serveur, vous invite à enregistrer la configuration et à redémarrer. Consultez <a href="#">Champs de configuration de l'Agent TS</a>, à la page 13.</li> <li>• Vous permet d'effectuer une mise à niveau vers cette version sans désinstaller la version précédente. Consultez <a href="#">Installer ou mettre à niveau l'Agent TS</a>, à la page 11.</li> <li>• Renommer le champ de configuration <b>Exclude Port(s)</b> (Exclure port[s]) en <b>Reserve Port(s)</b> (Réserver port[s]). Consultez <a href="#">Champs de configuration de l'Agent TS</a>, à la page 13.</li> <li>• Prise en charge des ports éphémères. Consultez <a href="#">Champs de configuration de l'Agent TS</a>, à la page 13.</li> <li>• La page de l'onglet <b>Monitor</b> (Surveiller) vous avertit lorsque plus de 50 % des ports TCP ou UDP ont été utilisés pour une session particulière. Consultez <a href="#">Afficher les informations sur l'Agent TS</a>, à la page 21.</li> <li>• Les plages de ports de session utilisateur attribuées selon la base du moins récemment utilisées. Consultez <a href="#">À propos de l'Agent Terminal Services (TS)</a>, à la page 1.</li> <li>• Vous permet d'exporter des informations de dépannage vers un fichier XML. Consultez <a href="#">Afficher les informations sur l'Agent TS</a>, à la page 21.</li> <li>• Vous permet de refluer les sessions utilisateur sur le FMC. Consultez <a href="#">Afficher les informations sur l'Agent TS</a>, à la page 21.</li> <li>• Tentative de fin de toutes les sessions utilisateur lorsque Agent TS est désinstallé. Consultez <a href="#">Désinstallation de l'Agent TS</a>, à la page 26.</li> </ul>	1.2
<ul style="list-style-type: none"> <li>• Le nombre maximal de sessions d'utilisateur par défaut a été modifié de 200 à 30.</li> <li>• La plage de ports est passée de 200 ou plus à 5 000 ou plus</li> </ul> <p>Ces modifications sont toutes abordées dans <a href="#">Champs de configuration de l'Agent TS</a>, à la page 13.</p>	1.1

Fonctionnalités	Version
<p>Agent TS</p> <p>Fonctionnalité introduite. L'Agent TS permet aux administrateurs de suivre l'activité des utilisateurs à l'aide du mappage de port. L'Agent TS, lorsqu'il est installé sur un serveur de terminaux, affecte une plage de ports aux sessions utilisateur individuelles et les ports de cette plage aux connexions TCP et UDP dans la session utilisateur. Les systèmes utilisent des ports uniques pour identifier les connexions TCP et UDP individuelles par les utilisateurs sur le réseau.</p>	1.0



## CHAPITRE 2

# Installer et configurer l'ASA de l'Agent TS

- [Installer ou mettre à niveau l'Agent TS, à la page 11](#)
- [Démarrer l'interface de configuration de l'Agent TS, à la page 12](#)
- [Configurer l'Agent TS, à la page 12](#)
- [Création du rôle VDI REST, à la page 19](#)

## Installer ou mettre à niveau l'Agent TS

### Avant de commencer

- Confirmez que l'Agent TS est pris en charge dans votre environnement, comme décrit dans [Exigences en matière d'environnement de serveur et de système, à la page 2](#).
- Mettre fin à toutes les sessions utilisateur en cours, comme décrit dans [Mettre fin à une session d'utilisateur en cours, à la page 25](#).

### Procédure

**Étape 1** Connectez-vous à votre serveur en tant qu'utilisateur avec des privilèges d'administrateur.

**Étape 2** Téléchargez le paquet de l'Agent TS à partir du site d'assistance : [TSAgent-1.2.0.exe](#).

#### Remarque

Téléchargez la mise à jour directement à partir du site. Si vous transférez le fichier par courriel, il pourrait être corrompu.

**Étape 3** Faites un clic droit sur [TSAgent-1.2.0.exe](#), puis choisissez **Run as Administrator** (Exécuter en tant qu'administrateur).

**Étape 4** Cliquez sur **Install** (Installer) et suivez les invites pour installer ou mettre à niveau l'Agent TS. Vous devez redémarrer l'ordinateur avant de pouvoir utiliser l'Agent TS.

### Prochaine étape

- Confirmez que l'Agent TS fonctionne comme indiqué dans [Affichage de l'état du composant du service de l'Agent TS, à la page 25](#).

- Démarrez l'Agent TS comme indiqué dans l'[Démarrage et arrêt des processus de l'Agent TS](#), à la page 26.
- Configurer l'Agent TS comme indiqué dans [Configurer l'Agent TS](#), à la page 12.

**Remarque**

Si le programme d'installation de l'Agent TS signale que le cadre .NET a échoué, exécutez la mise à jour de Windows et réessayez d'installer de l'Agent TS.

## Démarrer l'interface de configuration de l'Agent TS

*cite*

S'il y a un raccourci Agent TS sur votre bureau, doublez cliquez sur celui-ci. Sinon, utilisez la procédure suivante pour lancer l'interface de configuration de l'Agent TS.

### Procédure

**Étape 1** Connectez-vous à votre serveur en tant qu'utilisateur avec des privilèges d'administrateur.

**Étape 2** Ouvrez `C:\Program Files (x86)\Cisco\Terminal Services Agent`.

**Étape 3** Affichez les fichiers de programme pour l'Agent TS.

**Remarque**

Les fichiers de programme sont en affichage seulement. Ne supprimez pas, ne déplacez pas et ne modifiez pas ces fichiers.

**Étape 4** Double-cliquez sur le fichier `TSAgentApp` pour lancer l'Agent TS.

## Configurer l'Agent TS

Utilisez l'interface Agent TS pour configurer l'Agent TS. Vous devez enregistrer vos modifications et redémarrer le serveur pour que vos modifications prennent effet.

### Avant de commencer

- Si vous vous connectez au système, configurez et activez un ou plusieurs domaines Active Directory ciblant les utilisateurs que votre serveur surveille, comme décrit dans le *Guide de configuration de Cisco Secure Firewall Management Center*.
- Si vous vous connectez au système, configurez un compte d'utilisateur avec des privilèges REST VDI. Vous devez créer le rôle REST VDI dans le FMC, comme indiqué dans [Création du rôle VDI REST](#), à la page 19.
- Si vous êtes déjà connecté au système et que vous mettez à jour votre configuration Agent TS pour vous connecter à un autre FMC, vous devez mettre fin à toutes les sessions utilisateur en cours avant

d'enregistrer la nouvelle configuration. Pour en savoir plus, consultez [Mettre fin à une session d'utilisateur en cours](#), à la page 25 .

- Vous devez synchroniser l'heure sur votre serveur avec l'heure affichée sur l'Agent TS.
- Passez en revue et comprenez les champs de configuration, comme décrit dans [Champs de configuration de l'Agent TS](#) , à la page 13.

## Procédure

- 
- Étape 1** Sur le serveur où vous avez installé l'Agent TS, démarrez l'Agent TS comme décrit dans [Démarrer l'interface de configuration de l'Agent TS](#) , à la page 12.
- Étape 2** Cliquez sur **Configurer** (configurer).
- Étape 3** Accédez à la section des paramètres généraux de la page de l'onglet.
- Étape 4** Entrez une valeur pour **Max User Sessions** (Nombre maximal de sessions d'utilisateurs).
- Étape 5** Choisissez la **carte réseau du serveur** à utiliser pour la traduction de ports et les communications.
- Si l'adresse IP du serveur change ultérieurement, vous êtes invité à enregistrer la configuration et à redémarrer le serveur pour que la modification entre en vigueur.
- Étape 6** Entrez les valeurs **System Ports** (Ports système) et **User Ports** (Ports utilisateur). Dans une configuration valide, les plages de ports système et d'utilisateur ne se chevauchent pas.
- Étape 7** Saisissez les valeurs (Exclure port[s]) **Reserve Port(s)** (Réserver port[s]) sous la forme d'une liste séparée par des virgules.
- Les champs (Exclure port[s]) **Reserve port(s)** (Réserver port[s]) sont automatiquement remplis avec les valeurs attendues pour les ports du client Citrix MA (2598), du et du serveur de terminaux Windows (3389). Vous devez exclure les ports du client Citrix MA et du serveur de terminaux Windows.
- Étape 8** Accédez à la section des paramètres de connexion de l'API REST de l'onglet.
- Étape 9** Saisissez les valeurs de **Hostname/IP Address** (Nom d'hôte/Adresse IP) et **Port**
- Le FMC requiert le **Port** 443.
- Étape 10** Entrez le **nom d'utilisateur** et le **mot de passe**.
- Étape 11** Répétez les étapes 9 et 10 de la deuxième ligne de champs pour configurer une connexion de secours (basculement).
- Étape 12** Cliquez sur **Test** (Tester) pour tester la connexion API REST entre l'Agent TS et le système.
- Si vous avez configuré un FMC principal et secondaire, le test de connexion avec le secondaire échoue. Il s'agit du comportement attendu. L'Agent TS communique avec le FMC actif en tout temps. Si le principal est défaillant et devient le FMC inactif, l'Agent TS communique avec le FMC (qui est maintenant actif).
- Étape 13** Cliquez sur **Save** (Enregistrer) et confirmez que vous souhaitez redémarrer le serveur.
- 

## Champs de configuration de l'Agent TS

Les champs suivants sont utilisés pour configurer les paramètres sur un Agent TS.

## Paramètres généraux

Tableau 1 : Champs des paramètres généraux

Champ	Description	Exemple
(Exclure port[s]) Reserve Port(s) (Réserver port[s])	<p>Le ou les ports que vous souhaitez que l'Agent TS ignore. Saisissez les ports que vous souhaitez exclure sous forme de liste séparée par des virgules.</p> <p>L'Agent TS remplit automatiquement les champs (Exclure port[s]) <b>Reserve Port(s)</b> (Réserver port[s]) avec les valeurs de port par défaut pour le client Citrix MA (2598), le serveur de terminaux Windows (3389). Si vous n'excluez pas les ports appropriés, les applications nécessitant ces ports peuvent échouer.</p> <p><b>Remarque</b> Si un processus sur votre serveur utilise un port qui ne se trouve pas dans votre plage <b>System Ports</b> (Ports système) ou écoute sur celui-ci, vous devez exclure manuellement ce port à l'aide du champ (Exclure port[s]) <b>Reserve Port(s)</b> (Réserver port[s]).</p> <p><b>Remarque</b> Si une application cliente est installée sur votre serveur et que l'application est configurée pour se lier à un connecteur à l'aide d'un numéro de port précis, vous devez utiliser le champ (Exclure port[s]) <b>Reserve Port(s)</b> (Réserver port[s]) pour exclure ce port de la traduction.</p>	<p>Généralement, l'un des éléments suivants :</p> <ul style="list-style-type: none"> <li>• 2598, 3389 (les ports du client Citrix MA et du serveur de terminaux Windows)</li> </ul>
Nombre maximal de sessions par utilisateur	<p>Le nombre maximal de sessions d'utilisateur que vous souhaitez que l'Agent TS surveille. Un seul utilisateur peut exécuter plusieurs sessions d'utilisateur à la fois.</p> <p>Cette version de l'Agent TS prend en charge 29 sessions utilisateur par défaut, jusqu'à un maximum de 199 sessions utilisateur.</p>	29 (la valeur maximale prise en charge dans cette version de l'Agent TS)

Champ	Description	Exemple
Carte réseau du serveur	<p>Cette version de l'Agent TS prend en charge l'utilisation d'un contrôleur d'interface réseau (NIC) unique pour la traduction de ports et les communications entre systèmes de serveurs. Si au moins deux cartes réseau valides sont présentes sur votre serveur, l'Agent TS effectue la traduction de port uniquement sur l'adresse que vous précisez lors de la configuration.</p> <p>L'Agent TS remplit automatiquement ce champ avec l'adresse IPv4 et/ou l'adresse IPv6 de chaque carte d'interface réseau sur le serveur sur lequel le Agent TS est installé. Une carte réseau valide doit avoir une adresse IPv4 ou IPv6 unique, ou une de chaque type; une carte réseau valide ne peut pas avoir plusieurs adresses du même type.</p> <p><b>Remarque</b> Si l'adresse IP du serveur change, vous êtes invité à enregistrer la configuration et à redémarrer le serveur pour que la modification entre en vigueur.</p> <p><b>Remarque</b> Vous devez désactiver les messages d'annonce du routeur sur tous les appareils connectés à votre serveur. Si les annonces de routeur sont activées, les appareils peuvent attribuer plusieurs adresses IPv6 aux NIC sur votre serveur et invalider les NIC pour une utilisation avec l'Agent TS.</p>	Ethernet 2 (192.0.2.1) (une carte d'interface réseau sur votre serveur)

Champ	Description	Exemple
Ports du système	<p>La plage de ports que vous utilisez pour les processus système. L'Agent TS ignore cette activité. Configurez un port <b>Start</b> (Début) pour indiquer où vous souhaitez commencer la plage. Configurez une valeur <b>Range</b> (Plage) pour indiquer le nombre de ports que vous souhaitez désigner pour chaque processus système individuel.</p> <p>Cisco recommande une valeur <b>Range</b> (Plage) de de 5000 ou plus. Si vous remarquez que l'Agent TS manque fréquemment de ports pour les processus système, augmentez votre valeur <b>Range</b> (Plage).</p> <p><b>Remarque</b> Si un processus système nécessite un port qui ne correspond pas à vos <b>System ports</b> (Ports système) désignés, ajoutez le port au champ <b>Exclude port(s)</b> (Exclure port[s]). Si vous n'identifiez pas un port utilisé par les processus système dans la plage <b>System Ports</b> (Ports système) ou si vous ne l'excluez pas, les processus système peuvent échouer.</p> <p>L'Agent TS remplit automatiquement la valeur <b>End</b> (Fin) à l'aide de la formule suivante :</p> $([Start\ value] + [Range\ value]) - 1$ <p>Si vos entrées font que la valeur <b>End</b> (Fin) dépasse la valeur <b>Start</b> (Début) de <b>User Ports</b> (Ports utilisateurs), vous devez ajuster vos valeurs <b>Start</b> (Début) et <b>Range</b> (Plage).</p>	<p><b>Start</b> (Début) défini sur 10000 et <b>Range</b> (Plage) défini sur 5000</p>

Champ	Description	Exemple
Ports utilisateur	<p>La plage de ports que vous souhaitez désigner pour les utilisateurs. Configurez un port <b>Start</b> (Début) pour indiquer où vous souhaitez commencer la plage. Configurez une valeur <b>Range</b> (Plage) pour indiquer le nombre de ports que vous souhaitez désigner pour les connexions TCP ou UDP dans chaque session utilisateur individuelle.</p> <p><b>Remarque</b> Le trafic ICMP est transmis sans mappage de port.</p> <p>Cisco recommande une valeur <b>Range</b> (Plage) de de 1000 ou plus. Si vous remarquez que l'Agent TS manque fréquemment de ports pour le trafic utilisateur, augmentez votre valeur <b>Range</b> (Plage).</p> <p><b>Remarque</b> Lorsque le nombre de ports utilisés dépasse la valeur de <b>Range</b> (Plage), le trafic utilisateur est bloqué.</p> <p>L'Agent TS remplit automatiquement la valeur <b>End</b> (Fin) à l'aide de la formule suivante :</p> $[\text{Start value}] + ( [\text{Range value}] * [\text{Max User Sessions value}] ) - 1$ <p>Si vos entrées font que la valeur <b>End</b> (Fin) dépasse 65535, vous devez ajuster vos valeurs <b>Start</b> (Début) et <b>Range</b> (Plage).</p>	<p><b>Start</b> (Début) défini sur <b>15000</b> et <b>Range</b> (plage) défini sur <b>1000</b></p>
Ports éphémères	<p>Saisissez une plage de ports éphémères (également appelés <i>ports dynamiques</i>) pour permettre à l'Agent TS de faire la surveillance.</p>	<p><b>Start</b> (Début) défini sur <b>49152</b> et <b>Range</b> (Plage) défini sur <b>16384</b></p>

Champ	Description	Exemple
Communication avec le trafic inconnu	<p>Cochez la case <b>Permit</b> (Autoriser) pour permettre à l'Agent TS d'autoriser le trafic sur les ports système; cependant, l'Agent TS ne fait pas le suivi de l'utilisation du port. Les ports système sont utilisés par le compte de système local ou d'autres comptes d'utilisateurs locaux. (Un compte d'utilisateur local existe uniquement sur le serveur de l'Agent TS; il n'a pas de compte Active Directory correspondant.) Vous pouvez choisir cette option pour autoriser les types de trafic suivants :</p> <ul style="list-style-type: none"> <li>• Autorisez le trafic exécuté par le compte de système local (comme Server Message Block (SMB)) au lieu de le bloquer. Le FMC identifie ce trafic comme provenant de l'utilisateur Inconnu, car l'utilisateur n'existe pas dans Active Directory.</li> </ul> <p>L'activation de cette option vous permet également de tester avec succès la connexion avec le FMC si vous vous connectez au serveur de l'Agent TS à l'aide d'un compte de système local.</p> <ul style="list-style-type: none"> <li>• Lorsqu'une session d'utilisateur ou de système épuise tous les ports disponibles de sa plage, l'Agent TS autorise le trafic sur les ports éphémères. Cette option active le trafic; le FMC identifie le trafic comme provenant de l'utilisateur inconnu.</li> </ul> <p>Cela est particulièrement utile lorsque les ports système sont nécessaires pour maintenir le système en bon état, par exemple pour les mises à jour de contrôleur de domaine, les authentifications, les requêtes d'interface de gestion de fenêtres (WMI), etc.</p> <p>Décocher la case pour bloquer le trafic sur les ports du système.</p>	S.O.

### Paramètres de connexion de l'API REST

Vous pouvez configurer un appareil de système principal de connexion et, éventuellement, des appareils de système de secours (basculement) :

- Si votre appareil de système est autonome, laissez la deuxième ligne de champs de connexion de l'API REST vide.
- Si votre appareil de système est déployé avec un appareil de secours (basculement), utilisez la première ligne pour configurer une connexion à l'appareil principal et la deuxième ligne pour configurer une connexion à l'appareil de secours (basculement).

Tableau 2 : Champs des paramètres de connexion à l'API REST

Champ	Description	Exemple
Nom de domaine/adresse IP	Le nom d'hôte ou l'adresse IP de l'appliance du système.	192 . 0 . 2 . 1
Port	Le port utilisé par le système pour les communications de l'API REST. (Le FMC utilise généralement le port 443.)	443
Nom d'utilisateur et mot de passe	Les informations d'authentification pour la connexion. <ul style="list-style-type: none"> <li>Le système requiert un nom d'utilisateur et un mot de passe pour un utilisateur disposant de privilèges REST VDI sur le FMC. Pour en savoir plus sur la configuration de cet utilisateur, consultez le <i>Guide de configuration de Cisco Secure Firewall Management Center</i>.</li> </ul>	S.O.

## Création du rôle VDI REST

Pour connecter l'Agent TS au FMC, votre utilisateur doit avoir le rôle REST VDI. Le VDI REST n'est pas défini par défaut. Vous devez créer le rôle et l'attribuer à tout utilisateur utilisé dans la configuration de l'Agent TS.

Pour en savoir plus sur les utilisateurs et les rôles, consultez le *Guide de configuration de Cisco Secure Firewall Management Center*.

### Procédure

- 
- Étape 1** Connectez-vous au FMC en tant qu'utilisateur disposant des autorisations pour créer des rôles.
- Étape 2** Cliquez sur **System > Users** (Système > Utilisateurs).
- Étape 3** Cliquez sur l'onglet **Rôles d'utilisateur**.
- Étape 4** Dans la page de l'onglet User Roles (Rôles d'utilisateur), cliquez sur **Create User Role** (Créer le rôle d'utilisateur).
- Étape 5** Dans le champ Name (nom), saisissez `REST VDI`.  
Le nom du rôle n'est pas sensible à la casse.
- Étape 6** Dans la section enu-Based Permissions (Autorisations basées sur le menu), cochez **REST VDI** et assurez-vous que la case **Modify REST VDI** (Modifier REST VDI) est également cochée.
- Étape 7** Cliquez sur **Save** (enregistrer).
- Étape 8** Attribuez le rôle à l'utilisateur utilisé dans la configuration de l'Agent TS.
-





## CHAPITRE 3

# Afficher les données de l'Agent TS

- [Afficher les informations sur l'Agent TS, à la page 21](#)
- [Afficher l'état de la connexion, à la page 22](#)
- [Afficher les données de l'utilisateur, de la session utilisateur et de connexion TCP/UDP de l'Agent TS sur le FMC, à la page 23](#)

## Afficher les informations sur l'Agent TS

Utilisez la procédure suivante pour afficher les sessions utilisateur actuelles sur le réseau et les plages de ports attribuées à chaque session. Les données sont en lecture seule.

### Procédure

- Étape 1** Sur le serveur où vous avez installé l'Agent TS, démarrez l'interface de l'Agent TS comme décrit dans [Démarrer l'interface de configuration de l'Agent TS](#), à la page 12.
- Étape 2** Cliquez sur l'onglet **Monitor** (Surveiller). Les colonnes suivantes s'affichent :
- **REST Server ID** : nom d'hôte ou adresse IP du FMC qui signale les informations. Ces renseignements sont utiles si vous avez une configuration à haute disponibilité.
  - **Source IP** (IP source) : affiche la valeur de l'adresse IP de l'utilisateur au format IPv4 ou IPv6. Lorsque les adresses IPv4 et IPv6 sont configurées et qu'une nouvelle session vient d'être créée, les adresses IPv4 et IPv6 s'affichent sur des lignes distinctes.
  - **Status** (État) : affiche l'état de l'attribution de ports à l'utilisateur. Pour en savoir plus, consultez [Afficher l'état de la connexion, à la page 22](#).
  - **Session ID** (ID de session) : numéro qui identifie la session de l'utilisateur. Un utilisateur peut avoir plusieurs sessions à la fois.
  - **Username** (Nom d'utilisateur) : nom d'utilisateur associé à la session.
  - **Domain** (Domaine) : domaine Active Directory auquel l'utilisateur est connecté.
  - **Port Range** : plage de ports attribuée à l'utilisateur. (Une valeur de 0 indique un problème d'attribution de ports; pour en savoir plus, consultez [Afficher l'état de la connexion, à la page 22](#)).
  - **TCP Ports Usage** (Utilisation des ports TCP) et **UDP Ports Usage** (Utilisation des ports UDP): affiche le pourcentage de ports alloués par utilisateur. Lorsque le pourcentage dépasse 50 %, l'arrière-plan du champ est jaune. Lorsque le pourcentage dépasse 80 %, l'arrière-plan du champ est rouge.
  - **Login Date** (Date de connexion) : date à laquelle l'utilisateur est connecté.

## Étape 3

Le tableau suivant montre les actions que vous pouvez effectuer :

Article	Description
Cliquez sur un en-tête de colonne.	Triez les données du tableau en fonction de cette colonne.
	Saisissez une partie du nom d'utilisateur ou un nom d'utilisateur complet dans le champ de recherche <b>Filter by Username</b> (Filtrer par nom d'utilisateur).
	Cliquez sur cette page pour actualiser les sessions affichées sur cette page d'onglet.
	Exportez les informations de dépannage suivantes concernant l'Agent TS en tant que fichiers texte : <ul style="list-style-type: none"> <li>• Fichier XML contenant les données de configuration de l'Agent TS</li> <li>• Sortie de la commande <b>netstat -a -n -o</b></li> <li>• Liste des tâches de Windows</li> <li>• Liste des pilotes en cours d'exécution</li> </ul>
	Cochez la case à côté d'une ou plusieurs sessions pour celles-ci soient retransmises sur le FMC. Vous pouvez l'utiliser en cas de défaillance du service utilisateur sur le FMC.  Par exemple, supposons qu'un utilisateur se connecte au serveur de l'Agent TS après la défaillance du service utilisateur sur le FMC. Vous pouvez utiliser cette option pour renvoyer la session utilisateur après la restauration du service utilisateur. Cela devrait entraîner l'affichage du mot <b>Success</b> (Réussite) pour cet utilisateur dans la colonne Status (État).

## Afficher l'état de la connexion

Lorsque les utilisateurs se sont connectés aux services de terminaux sur lesquels l'Agent TS est installé, une nouvelle session système est créée, une plage de ports est attribuée à cette session et les résultats sont envoyés à FMC pour propagation vers les appareils gérés.

La page de l'onglet Monitor (Surveiller) vous permet de confirmer que la plage de ports a bien été envoyée à FMC. Voici quelques-unes des raisons pour lesquelles le processus a peut-être échoué :

- Problèmes de connexion réseau
  - Identifiants VDI non valides
- Expiration du jeton
- Nom de domaine configuré pour le mauvais domaine

## Procédure

- 
- Étape 1** Sur le serveur où vous avez installé l'Agent TS, démarrez l'interface de l'Agent TS comme décrit dans [Démarrer l'interface de configuration de l'Agent TS](#), à la page 12.
- Étape 2** Cliquez sur l'onglet **Monitor** (Surveiller).
- Étape 3** La colonne Status (État) comporte l'une des valeurs suivantes :
- **Pending** (En attente) : l'action est en attente, mais pas encore terminée.
  - **Failed** (Échec) : l'action a échoué. Cliquez sur le mot **Failed** (Échec) pour afficher un message d'erreur. Si l'erreur indique un échec de communication avec le FMC, essayez de rediriger le trafic pour cette session, comme indiqué dans [View Information About the TS Agent](#) (Afficher les informations sur l'Agent TS).
  - **Success** (Réussite) : l'action a bien été exécutée.
- 

# Afficher les données de l'utilisateur, de la session utilisateur et de connexion TCP/UDP de l'Agent TS sur le FMC

Utilisez la procédure suivante pour afficher les données signalées par l'Agent TS. Pour en savoir plus à propos des tableaux de FMC, consultez le *Guide de configuration de Cisco Secure Firewall Management Center*.

## Procédure

- 
- Étape 1** Connectez-vous au FMC où vous avez configuré les domaines ciblant les utilisateurs que votre serveur surveille.
- Étape 2** Pour afficher les utilisateurs dans le tableau Users (Utilisateurs), choisissez **Analysis > Users > Users** (Analyse, Utilisateurs, Utilisateurs). Le FMC remplit les colonnes **Current IP** (IP actuelle), **End Port** (Port de fin), and **Start Port** (Port de début) si la session d'un utilisateur de l'Agent TS est actuellement active.
- Étape 3** Pour afficher les sessions d'utilisateur dans le tableau d'activité des utilisateurs, sélectionnez **Analysis > Users > User Activity** (Analyse, Utilisateurs, Activité des utilisateurs). Le FMC remplit les colonnes **Current IP** (IP actuelle), **End Port** (Port de fin), and **Start Port** (Port de début) si l'Agent TS a signalé la session utilisateur.
- Étape 4** Pour afficher les connexions TCP/UDP dans le tableau des événements de connexion, sélectionnez **Analysis > Connections > Events**(Analyse, Connexions, Événements). Le FMC remplit le champ **Initiator/Responder IP** (IP de l'initiateur/répondant) avec l'adresse IP de l'Agent TS qui a signalé la connexion ainsi que le champ **Source Port/ICMP Type** (Port de la source/type d'ICMP) et le port que l'Agent TS attribué à la connexion.
-





## CHAPITRE 4

# Gérer l'Agent TS

---

- [Mettre fin à une session d'utilisateur en cours](#), à la page 25
- [Affichage de l'état du composant du service de l'Agent TS](#), à la page 25
- [Démarrage et arrêt des processus de l'Agent TS](#), à la page 26
- [Affichage des journaux d'activité de l'Agent TS sur le serveur](#), à la page 26
- [Désinstallation de l'Agent TS](#), à la page 26

## Mettre fin à une session d'utilisateur en cours

Utilisez la procédure suivante pour déconnecter un utilisateur du réseau et mettre fin à la session.

### Procédure

---

- Étape 1** Connectez-vous à votre serveur d'Agent TS en tant qu'utilisateur avec des privilèges d'administrateur.
- Étape 2** Ouvrez **Start > > [All Programs] > Task Manager** (Démarrer > [Tous les programmes], Gestionnaire de tâches).
- Étape 3** Développez la fenêtre en cliquant sur **More Details** (Plus de détails).
- Étape 4** Cliquez sur l'onglet **Users** (Utilisateurs).
- Étape 5** (Facultatif) Pour informer un utilisateur que vous mettez fin à sa session, effectuez un clic droit sur la session utilisateur et choisissez **Send message** (Envoyer un message).
- Étape 6** Faites un clic droit sur la session utilisateur et choisissez **Sign off** (Se déconnecter).
- Étape 7** Cliquez sur **Sign out user** (Déconnecter l'utilisateur) pour confirmer l'action.
- 

## Affichage de l'état du composant du service de l'Agent TS

Utilisez la procédure suivante pour confirmer que le composant de service de l'Agent TS est en cours d'exécution. Pour plus d'informations sur le composant de service, consultez [À propos de l'Agent Terminal Services \(TS\)](#), à la page 1.

## Procédure

- 
- Étape 1** Connectez-vous à votre serveur en tant qu'utilisateur avec des privilèges d'administrateur.
- Étape 2** Ouvrez **Start > Tools > Services** (Démarrer, Outil, Services).
- Étape 3** Localisez `CiscoTSAgent` (Agent TS Cisco) et consultez le **Status** (État).
- Étape 4** (Facultatif) Si le composant de service Agent TS est arrêté, démarrez le service Agent TS comme décrit dans [Démarrage et arrêt des processus de l'Agent TS](#), à la page 26.
- 

# Démarrage et arrêt des processus de l'Agent TS

Utilisez la procédure suivante pour démarrer ou arrêter le composant de service de l'Agent TS.

## Procédure

- 
- Étape 1** Connectez-vous à votre serveur en tant qu'utilisateur avec des privilèges d'administrateur.
- Étape 2** Ouvrez **Start > Administrative Tools > Services** (Démarrer, Outils administratifs, services).
- Étape 3** Accédez au `CiscoTSAgent` et cliquez avec le bouton droit pour accéder au menu contextuel.
- Étape 4** Choisissez **Start** (Démarrer) ou **Stop** (Arrêter) pour démarrer ou arrêter le service Agent TS.
- 

# Affichage des journaux d'activité de l'Agent TS sur le serveur

Si le service d'assistance vous le demande, utilisez la procédure suivante pour afficher les journaux d'activité du composant du service.

## Procédure

---

Ouvrez **Tools > Event Viewer > Applications and Services Log > Terminal Services Agent Log** (Outils, Visualisateur d'événement, Journal des applications et des services, Journal des agents des services de terminaux).

---

# Désinstallation de l'Agent TS

Utilisez la procédure suivante pour désinstaller l'Agent TS de votre serveur. La désinstallation de l'Agent TS supprime l'interface, le service et le pilote de votre serveur. La désinstallation de l'Agent TS met également fin aux sessions utilisateur actives, comme indiqué au FMC. La modification de la cryptographie forte n'est pas supprimée.

## Procédure

- 
- Étape 1** Connectez-vous à votre serveur en tant qu'utilisateur avec des privilèges d'administrateur.
- Étape 2** Ouvrez **Start > Control Panel** (Démarrer, Panneau de contrôle).
- Étape 3** Cliquez sur **All Control Panel Items > Programs and Features** (Tous les éléments du panneau de commande, Programmes et fonctionnalités).
- Étape 4** Faites un clic droit sur **Terminal Services Agent** (Agent des services de terminaux) et choisissez **Uninstall** (Désinstaller).
-



## À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d'incohérence, la version anglaise du présent contenu prévaudra.