



Contrôle de l'utilisateur à l'aide de l'agent TS

Pour utiliser l'agent TS comme source d'identité pour la sensibilisation et le contrôle des utilisateurs, installez et configurez le logiciel agent TS comme indiqué dans la section [Guide des agents de Cisco Terminal Services \(TS\)](#).

Prochaine étape :

- Précisez les utilisateurs à contrôler et d'autres options à l'aide d'une politique d'identité, comme décrit dans [Créer une politique d'identité](#).
- Associez la règle d'identité à une politique de contrôle d'accès, qui filtre et inspecte éventuellement le trafic, comme indiqué dans [Association d'autres politiques au contrôle d'accès](#).
- Déployez vos politiques de contrôle d'identité et de contrôle d'accès sur les périphériques gérés, comme indiqué dans [Déployer les modifications de configuration](#).
- Surveillez l'activité de l'utilisateur,
- [La source d'identité de l'agent des services de terminaux \(TS\), à la page 1](#)
- [Directives pour les agents TS, à la page 2](#)
- [Contrôle de l'utilisateur à l'aide de l'agent TS, à la page 2](#)
- [Dépannage de la source d'identité de l'agent TS, à la page 2](#)
- [Historique de l'agent TS, à la page 3](#)

La source d'identité de l'agent des services de terminaux (TS)

L'agent TS est une méthode d'authentification passive et l'une des sources d'identité officielles prises en charge par le système. Un serveur de terminaux Windows effectue l'authentification et l'agent des services TS le signale à un centre de gestion autonome ou à haute disponibilité.

Lorsqu'il est installé sur des serveurs de terminaux Windows, l'agent TS affecte une plage de ports unique aux utilisateurs individuels lorsqu'ils se connectent ou se déconnectent d'un réseau surveillé. Le centre de gestion utilise le port unique pour identifier les utilisateurs individuels dans le système. Vous pouvez utiliser un agent TS pour surveiller l'activité d'un utilisateur sur un serveur de terminaux Windows et envoyer des données chiffrées à centre de gestion.

L'agent TS ne signale pas les tentatives de connexion en échec. Les données obtenues à partir de l'agent TS peuvent être utilisées pour la sensibilisation et le contrôle de l'utilisateur.

Directives pour les agents TS

L'agent TS nécessite une configuration en plusieurs étapes et comprend les éléments suivants :

1. Un serveur de terminaux Windows sur lequel l'agent TS est installé et configuré.
2. Un ou plusieurs domaines d'identité ciblant les utilisateurs que votre serveur surveille.

Vous installez l'agent TS sur un serveur de terminaux Microsoft Windows. Pour des informations détaillées sur l'installation et la configuration en plusieurs étapes de l'agent TS, ainsi qu'une explication complète du serveur et des exigences du système Firepower, consultez [Guide des agents de Cisco Terminal Services \(tS\)](#).

Les données des agents TS sont visibles dans les tableaux Utilisateurs, Activité des utilisateurs et Événement de connexion et peuvent être utilisées pour la sensibilisation et le contrôle de l'utilisateur.

**Remarque**

Si l'agent TS surveille les mêmes utilisateurs qu'une autre source d'identité avec authentification passive (ISE/ISE-PIC), centre de gestion priorise les données de l'agent TS. Si l'agent TS et une autre source d'identité passive signalent une activité par la même adresse IP, seules les données de l'agent sont enregistrées dans centre de gestion.

Contrôle de l'utilisateur à l'aide de l'agent TS

Pour utiliser l'agent TS comme source d'identité pour la sensibilisation et le contrôle des utilisateurs, installez et configurez le logiciel agent TS comme indiqué dans la section [Guide des agents de Cisco Terminal Services \(tS\)](#).

Prochaine étape :

- Précisez les utilisateurs à contrôler et d'autres options à l'aide d'une politique d'identité, comme décrit dans [Créer une politique d'identité](#).
- Associez la règle d'identité à une politique de contrôle d'accès, qui filtre et inspecte éventuellement le trafic, comme indiqué dans [Association d'autres politiques au contrôle d'accès](#).
- Déployez vos politiques de contrôle d'identité et de contrôle d'accès sur les périphériques gérés, comme indiqué dans [Déployer les modifications de configuration](#).
- Surveillez l'activité de l'utilisateur.

Dépannage de la source d'identité de l'agent TS

Pour d'autres renseignements relatifs au dépannage, consultez [Résoudre les problèmes liés aux domaines et aux téléchargements d'utilisateurs](#) et [Dépannage du contrôle d'utilisateur](#).

Si vous rencontrez des problèmes avec l'intégration de l'agent TS, vérifiez les éléments suivants :

- Vous devez synchroniser l'heure sur votre serveur d'agent TS avec l'heure affichée sur centre de gestion.

- Si l'agent TS surveille les mêmes utilisateurs qu'une autre source d'identité avec authentification passive (ISE/ISE-PIC), centre de gestion priorise les données de l'agent TS. Si l'agent TS et une source d'identité passive signalent une activité par la même adresse IP, seules les données de l'agent TS sont enregistrées dans centre de gestion.
- Les sessions FTP actives sont affichées comme utilisateur **Unknown** dans les événements. Cette situation est normale car, dans le protocole FTP actif, c'est le serveur (et non le client) qui lance la connexion et aucun nom d'utilisateur ne devrait être associé au serveur FTP. Pour plus d'informations sur le FTP actif, consultez [RFC 959](#).

Pour plus de renseignements sur le dépannage, consultez [Guide des agents de Cisco Terminal Services \(TS\)](#).

Historique de l'agent TS

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
L'agent TS communique avec Cisco Defense Orchestrator	N'importe lequel	7.2.0	En appliquant un jeton de Cisco Defense Orchestrator, l'agent TS des services peut obtenir des sessions de connexion d'utilisateur de la même manière que pour Cisco Defense Orchestrator.
Agent TS pour le contrôle de l'utilisateur.	N'importe lequel	6.2.0	<p>Fonctionnalité introduite. Firepower offre désormais la possibilité de mieux identifier les utilisateurs individuels dans des environnements partagés, tels que Virtual Desktop Infrastructure (VDI) de Citrix, afin d'appliquer avec précision les règles de politique basées sur l'utilisateur sur le pare-feu. Les utilisateurs sont identifiés par les ports utilisés.</p> <p>Le logiciel agent des services TS est mis à jour indépendamment du centre de gestion Cisco Firepower Management Center. Pour obtenir plus de renseignements, consultez la section :</p> <ul style="list-style-type: none"> • Guide des agents de Cisco Terminal Services (TS) disponible sur cisco.com • Guide de compatibilité de Cisco Firepower

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.