TS エージェントによるユーザーの制御

TS エージェントをユーザー認識およびユーザー制御用のアイデンティティソースとして使用するには、Cisco ターミナルサービス（TS）エージェントガイドの説明に従って TS エージェントソフトウェアをインストールして設定します。

次に行う作業：

- アイデンティティ ポリシーの作成の説明に従って、制御するユーザーおよび他のオプションを、アイデンティティ ポリシーを使って指定します。
- アクセス制御への他のポリシーの関連付けの説明に従って、アイデンティティ ルールをアクセス コントロール ポリシーに関連付けます。このポリシーは、トラフィックをフィルタし、オプションで検査します。
- 設定変更の展開の説明に従って、使用するアイデンティティ ポリシーとアクセス コントロール ポリシーを管理対象デバイスに展開します。
- Cisco Secure Firewall Management Center アドミニストレーション ガイド の「*Using Workflows*」の説明に従って、ユーザーアクティビティをモニターします。

ターミナルサービス（TS）エージェントのアイデンティティ ソース

TS エージェントはパッシブ認証方式であり、システムでサポートされる権限のあるアイデンティティソースの 1 つです。Windows Terminal Server が認証を実行し、TS エージェントがスタンドアロンまたはハイ アベイラビリティの Management Center にその認証の実行を報告します。

TS エージェントは、Windows Terminal Server にインストールされると、個々のユーザーがモニター対象ネットワークにログインまたはログアウトする際にそのユーザーに固有のポート範囲を割り当てます。Management Center では、この固有のポートを使用してシステムの個々のユーザーを識別します。1 つの TS エージェントを使用して、1 つの Windows Terminal Server 上のユーザ アクティビティをモニタし、暗号化データを Management Center に送信できます。

TS エージェントは失敗したログイン試行を報告しません。TS エージェントから取得されたデータは、ユーザー認識とユーザー制御に使用できます。

TS エージェントのガイドライン

TS エージェントには段階的な設定が必要で、次のものがあります。

1. TS エージェントがインストールおよび設定された Windows Terminal Server。
2. サーバがモニタするユーザを対象とする 1 つ以上のアイデンティティ レルム。

TS エージェントは、Microsoft Windows Terminal Server にインストールします。段階的な TS エージェントのインストールと設定、およびサーバーとシステムの要件の詳細については、Cisco ターミナルサービス（TS）エージェントガイド を参照してください。

TS エージェントのデータは [ユーザー（Users）] テーブル、[ユーザー アクティビティ（User Activity）] テーブル、および [接続イベント（Connection Event）] テーブルに表示され、ユーザー認識とユーザー制御に使用できます。

（注） TS エージェントが別のパッシブ認証の ID ソース（ISE/ISE-PIC）と同じユーザーをモニターしている場合、Management Center は TS エージェントのデータを優先します。同じ IP アドレスによるアクティビティが TS エージェントと別のパッシブ アイデンティティ ソースから報告される場合、TS エージェントのデータだけが Management Center に記録されます。

TS エージェントによるユーザーの制御

TS エージェントをユーザー認識およびユーザー制御用のアイデンティティソースとして使用するには、Cisco ターミナルサービス（TS）エージェントガイドの説明に従って TS エージェントソフトウェアをインストールして設定します。

次に行う作業：

- アイデンティティ ポリシーの作成の説明に従って、制御するユーザーおよび他のオプションを、アイデンティティ ポリシーを使って指定します。
- アクセス制御への他のポリシーの関連付けの説明に従って、アイデンティティ ルールをアクセス コントロール ポリシーに関連付けます。このポリシーは、トラフィックをフィルタし、オプションで検査します。

- 設定変更の展開の説明に従って、使用するアイデンティティ ポリシーとアクセス コントロール ポリシーを管理対象デバイスに展開します。
- Cisco Secure Firewall Management Center アドミニストレーション ガイド の「*Using Workflows*」の説明に従って、ユーザーアクティビティをモニターします。

TS エージェント アイデンティティ ソースのトラブルシューティング

関連の他のトラブルシューティングについては、レルムとユーザーのダウンロードのトラブルシュートおよびユーザー制御のトラブルシューティングを参照してください。

TS エージェントの統合で問題が発生した場合は、次のことを確認してください。

- TS エージェントサーバーと Management Center の時計を同期させる必要があります。
- TS エージェントが別のパッシブ認証の ID ソース（ISE/ISE-PIC）と同じユーザーをモニターしている場合、Management Center は TS エージェントのデータを優先します。TS エージェントとパッシブ ID ソースが同じ IP アドレスによるアクティビティを報告した場合は、TS エージェントのデータのみが Management Center に記録されます。
- Active FTP sessions are displayed as the **Unknown** user in events. これは正常な処理です。アクティブ FTP では、（クライアントではない）サーバーが接続を開始し、FTP サーバーには関連付けられているユーザー名がないはずだからです。アクティブ FTP の詳細については、RFC 959 を参照してください。

トラブルシューティングの詳細については、Cisco ターミナルサービス（TS）エージェントガイドを参照してください。

TS エージェントの履歴

機能	最小 Management Center	最小 Threat Defense	詳細
ユーザ制御用の TS エージェント。	7.2.0	6.2.0	導入された機能。FirePOWER が、Citrix の仮想デスクトップ インフラストラクチャ（VDI）などの共有環境で個々のユーザをより正確に識別して、ファイアウォールにユーザ ベースのポリシー ルールを正確に適用できるようになりました。ユーザは使用されるポートによって識別されます。 TS エージェント ソフトウェアは、Firepower Management Center とは独立して更新されます。詳細については、以下を参照してください。 • cisco.com で利用可能な『*Cisco Terminal Services (TS) Agent Guide*』 • 『Cisco Firepower Compatibility Guide』

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。