



シスコ ターミナルサービス (TS) エージェントバージョン 1.3 ガイド

初版：2021年3月2日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター
0120-092-255 (フリーコール、携帯・PHS含む)

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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.

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)

© 2019 Cisco Systems, Inc. All rights reserved.



第 1 章

ターミナル サービス (TS) エージェントの概要

- シスコ ターミナル サービス (TS) エージェントについて (1 ページ)
- サーバおよびシステム環境要件 (2 ページ)
- Firepower Management Center での TS エージェントに関する問題のトラブルシューティング (4 ページ)
- TS エージェントに関する問題のトラブルシューティング (7 ページ)
- ユーザエージェントに関する問題のトラブルシューティング (9 ページ)
- 解決済みの問題 (9 ページ)
- TS エージェントの履歴 (10 ページ)

シスコターミナルサービス (TS) エージェントについて

シスコ ターミナル サービス (TS) エージェントを使用すると、Firepower Management Center または ISE/ISE-PIC では、Microsoft Windows ターミナル サーバによってモニタされるユーザトラフィックを一意に識別できるようになります。TS エージェントがない場合、システムは、Microsoft Windows ターミナルサーバからのすべてのトラフィックを、1 つの IP アドレスから発信された単一のユーザセッションとして認識します。



(注) 潜在的な問題を回避するとともに、ご使用のソフトウェアが最新であることを確保するため、シスコは、TS エージェントの最も新しくリリースされたバージョンを使用することを推奨します。最新バージョンを確認するには、<https://www.cisco.com/c/en/us/support/index.html> シスコ サポートのサイトを参照してください。

TS エージェントは、Microsoft Windows ターミナルサーバにインストールおよび設定されると、一定のポート範囲を個別のユーザセッションに割り当て、その範囲内のポートをユーザセッションにおける TCP および UDP 接続に割り当てます。システムは、ネットワーク上のユーザによる個別の TCP および UDP 接続を識別するために一意のポートを使用します。ポート範囲

は、Least Recently Used ベースで割り当てられます。つまり、ユーザセッションの終了後、同じポート範囲が新しいユーザセッションにすぐに再利用されることはありません。



(注) ICMP メッセージは、ポートマッピングなしで渡されます。

コンピュータのシステムコンテキスト内で実行されるサービスによって生成されるトラフィックは、TS エージェントによって追跡されません。特に、サーバメッセージブロック (SMB) トラフィックはシステム コンテキスト内で実行されるため、TS エージェントは、SMB トラフィックを識別しません。

TS エージェントは、TS エージェントホストごとに最大 199 の同時ユーザセッションをサポートします。単一のユーザが複数の同時ユーザセッションを実行している場合、TS エージェントは、個別のユーザセッションのそれぞれに一意のポート範囲を割り当てます。あるユーザがセッションを終了すると、TS エージェントは、そのポート範囲を別のユーザセッションに使用できます。

各 FMC は、同時に接続する最大 50 の TS エージェントをサポートします。

お使いのサーバにインストールされる TS エージェントには、3 つの主要コンポーネントがあります。

- インターフェイス：TS エージェントを設定し、現在のユーザセッションをモニタするアプリケーション
- サービス：ユーザのログインおよびログオフをモニタするプログラム
- ドライバ：ポート変換を行うプログラム

TS エージェントは次のいずれかに使用できます。

- Firepower Management Center 上の TS エージェント データは、ユーザ認識やユーザ コントロールに使用できます。Firepower システムでの TS エージェントデータの使用方法に関する詳細については、『Firepower Management Center Configuration Guide』を参照してください。



(注) TS エージェントをユーザ認識やユーザコントロールに使用するには、データの送信先を Firepower Management Center のみに設定する必要があります。詳細については、[TS エージェントの設定 \(14 ページ\)](#) を参照してください。

サーバおよびシステム環境要件

お使いのシステム上で TS エージェントをインストールして実行するには、次の要件を満たす必要があります。



- (注) 潜在的な問題を回避するとともに、ご使用のソフトウェアが最新であることを確保するため、シスコは、TS エージェントの最も新しくリリースされたバージョンを使用することを推奨します。最新バージョンを確認するには、<https://www.cisco.com/c/en/us/support/index.html> シスコ サポートのサイトを参照してください。

サーバ要件

64 ビット Microsoft Windows ターミナル サーバの次のバージョンのいずれかに TS エージェントをインストールします。

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2



- (注) TS エージェントのインストールには、サーバ上に 653 KB の空き領域が必要です。



- (注) TS エージェントサーバで Web トラフィックをプロキシするアンチウイルスソフトウェアを使用している場合、通常、ユーザトラフィックはシステムユーザに割り当てられ、FMC はそれらのユーザを不明なユーザとして認識します。この問題を回避するには、Web トラフィックのプロキシを無効にします。

TS エージェントは、サーバにインストールされるターミナル サービス ソリューションのうち、以下のものと同時に使用することができます。

- Citrix Provisioning
- Citrix XenDesktop
- Citrix XenApp
- Xen Project Hypervisor
- VMware vSphere Hypervisor/VMware ESXi 6.0
- Windows ターミナル サービス または Windows リモートデスクトップ サービス (RDS)

このバージョンの TS エージェントでは、ポート変換およびサーバシステム間の通信に、単一のネットワーク インターフェイス コントローラ (NIC) を使用することができます。サーバに有効な NIC が 2 つ以上存在する場合、TS エージェントは、設定の際に指定されたアドレスに対してのみポートの変換を実行します。有効な NIC には必ず、IPv4 もしくは IPv6 のアドレ

スが1つだけ、または各タイプのアドレスが1つずつあります。有効な NIC が同じ種類のアドレスを複数持つことはできません。



- (注) サーバに接続されているデバイスのいずれかでルータアドバタイズメントが有効になっていると、それらのデバイスがサーバ上の NIC に複数の IPv6 アドレスを割り当て、TS エージェントで使用する NIC を無効にしてしまう可能性があります。

Firepower システムの要件

このバージョンの TS エージェントは、バージョン 6.4 以降の Firepower システムを実行するスタンドアロンまたは高可用性の Firepower Management Center との接続をサポートします。

Firepower Management Center での TS エージェントに関する問題のトラブルシューティング

Firepower Management Center での TS エージェントに関する問題の詳細については、次の項を参照してください。

このリリースで解決された既知の問題の詳細については、[解決済みの問題 \(9 ページ\)](#) を参照してください。

Firepower Management Center がシステム プロセスについてはユーザ情報を表示しない

システム コンテキスト内で実行されるサービスによって生成されるトラフィックは、TS エージェントによって追跡されません。特に、次の点に注意してください。

- サーバメッセージブロック (SMB) トラフィックはシステムコンテキスト内で実行されるため、TS エージェントは SMB トラフィックを識別しません。
- 一部のアンチウイルス アプリケーションは、Web トラフィックをオンプレミスまたはクラウドゲートウェイにプロキシして、クライアントコンピュータに到達する前にウイルスを捕捉します。ただし、これは、アンチウイルスソフトウェアが通常はシステムアカウントを使用することを意味します。この場合、FMC はユーザを不明なユーザと見なします。この問題を解決するには、Web トラフィックプロキシを無効にします。

TS エージェント ユーザのタイムアウトが期待されるときに発生しない

サーバと Firepower Management Center の時計を同期させる必要があります。

TS エージェントがユーザセッション ポートの変換を実行しない

TS エージェントは、次の場合はポート変換を実行しません。

- ユーザセッションが、設定されている [最大ユーザセッション (Max User Sessions)] の値を超えている。たとえば、[最大ユーザセッション (Max User Sessions)] が 29 に設定

されている場合、TS エージェントは、30 番目のユーザセッションに対しては、ポート変換を実行しません。

- 使用可能なポートがすべて使用中。たとえば、[ユーザポート (User Ports)] の [範囲 (Range)] の値がユーザセッションごとに 1000 ポートに指定されている場合、TS エージェントは、1001 番目の TCP/UDP 接続に対しては、ユーザが別の TCP/UDP 接続を終了してポートを開放するまで、ポート変換を実行しません。
- ユーザセッションに関連付けられたドメインがない。たとえば、サーバ管理者のセッションが、ローカルシステムには認証されたものの外部の Active Directory サーバには認証されなかった場合、サーバ管理者は、サーバにログインしますがネットワークおよび TS エージェントにはアクセスできず、TS エージェントは、そのユーザセッションにポートを割り当てません。

TS エージェントがポート変換を期待されるように実行しない

サーバの IP アドレスを手動で編集する場合、TS エージェント上で [サーバ NIC (Server NIC)] を編集する必要があります。その後で、TS エージェント設定を保存し、サーバを再起動します。

ユーザセッションが Firepower Management Center に期待されるように報告されない

別の Firepower Management Center に接続するように TS エージェント設定を更新する場合は、新しい設定を保存する前に、現在のすべてのユーザセッションを終了する必要があります。詳細については、[現在のユーザセッションの終了 \(37 ページ\)](#) を参照してください。

クライアントアプリケーションのトラフィックがユーザトラフィックとして Firepower Management Center に報告される

サーバにクライアントアプリケーションがインストールされており、そのアプリケーションが、[システムポート (System Ports)] の範囲外のポートを使用するソケットにバインドするように設定されている場合、[除外ポート (Exclude Port(s))] フィールドを使用して、そのポートを変換から除外する必要があります。そのポートを除外しないと、そのポートが [ユーザポート (User Ports)] の範囲内である場合、TS エージェントは、そのポートでのトラフィックを、関係のないユーザトラフィックとして報告する可能性があります。

これを防ぐには、クライアントアプリケーションを、[システムポート (System Ports)] の範囲内のポートを使用するソケットにバインドするように設定します。

サーバアプリケーションのタイムアウト、ブラウザのタイムアウト、または TS エージェントと Firepower Management Center の間の接続障害

TS エージェントサーバ上のアプリケーションが TCP/UDP 接続を終了したものの、それに関連するポートが完全に閉じられていない場合、TS エージェントは、そのポートを変換に使用できません。サーバがポートを完全に閉じる前に TS エージェントがそのポートを変換に使用しようとする、接続は失敗します。



- (注) 完全に閉じられていないポートを特定するには、`netstat` コマンド (サマリー情報用) または `netstat -a -o -n -b` コマンド (詳細情報用) を使用できます。これらのポートのステータスは、`TIME_WAIT` または `CLOSE_WAIT` です。

この問題が発生する場合は、問題によって影響を受ける TS エージェント ポートの範囲を大きくします。

- 正しく閉じられていないポートが [ユーザポート (User Ports)] の範囲内である場合、サーバアプリケーションまたはブラウザのタイムアウトが発生します。
- 正しく閉じられていないポートが [システムポート (System Ports)] の範囲内である場合、TS エージェントと Firepower Management Center の間で接続障害が発生します。

TS エージェントと Firepower Management Center の間の接続障害

設定中に [テスト (Test)] ボタンをクリックしたときに TS エージェントが Firepower Management Center との接続を確立できなかった場合は、次のことを確認してください。

- 50 を超える TS エージェントクライアントが同時に FMC への接続を試行していないことを確認します。
- 入力した [ユーザ名 (Username)] と [パスワード (Password)] が、[REST VDI ロールの作成 \(31 ページ\)](#) で説明するように、REST VDI 特権を有する Firepower Management Center ユーザの正しいクレデンシャルであるか確認します。

TS エージェントからのユーザ認証が成功したかを確認するには、Firepower Management Center で監査ログを表示します。

- ハイアベイラビリティ設定で、設定の直後にセカンダリの Firepower Management Center への接続が失敗した場合、それは、想定されている動作です。TS エージェントは、アクティブな Firepower Management Center と常に通信します。

セカンダリがアクティブな Firepower Management Center となっている場合、プライマリの Firepower Management Center への接続は失敗します。

システム プロセスまたはサーバ上のアプリケーションが誤動作している

お使いのサーバ上のシステム プロセスが [システムポート (System Ports)] の範囲にないポートを使用またはリッスンしている場合、そのポートは、[除外ポート (Exclude Port(s))] フィールドを使用して手動で除外する必要があります。

お使いのサーバ上のアプリケーションが Citrix MA クライアントのポート (2598) または Windows ターミナルサーバのポート (3389) を使用またはリッスンしている場合、それらのポートが [除外ポート (Exclude Port(s))] フィールドで除外されていることを確認してください。

Firepower Management Center に TS エージェントからの不明なユーザが表示される

Firepower Management Center が TS エージェントからの不明なユーザを表示するのは、次の状況です。

- TS エージェントのドライバコンポーネントがクラッシュすると、ダウンタイム中に発生したユーザセッションは、Firepower Management Center のログに不明なユーザとして記録されます。
- 一部のアンチウイルス アプリケーションは、Web トラフィックをオンプレミスまたはクラウドゲートウェイにプロキシして、クライアントコンピュータに到達する前にウイルスを捕捉します。ただし、これは、アンチウイルスソフトウェアが通常はシステムアカウントを使用することを意味します。この場合、FMC はユーザを不明なユーザと見なします。この問題を解決するには、Web トラフィックプロキシを無効にします。
-
- ハイアベイラビリティ設定でプライマリの Firepower Management Center がダウンすると、フェールオーバー中の 10 分のダウンタイムの間に TS エージェントによって報告されるログインは、次のように処理されます。
 - Firepower Management Center で以前に見られたことのないユーザについて TS エージェントがユーザセッションデータを報告した場合、そのデータは、Firepower Management Center には、不明なユーザ アクティビティとして記録されます。
 - Firepower Management Center で以前に見られたことがあるユーザの場合、データは正常に処理されます。

ダウンタイム後、不明のユーザはアイデンティティ ポリシーのルールに従って再確認され、処理されます。

サーバの NIC リストに NIC が表示されない

サーバに接続されているデバイスで、ルータ アドバタイズメント メッセージを無効にする必要があります。ルータアドバタイズメントが有効になっていると、デバイスがサーバ上の NIC に複数の IPv6 アドレスを割り当て、TS エージェントで使用する NIC を無効にしてしまう可能性があります。

有効な NIC には必ず、IPv4 もしくは IPv6 のアドレスが 1 つだけ、または各タイプのアドレスが 1 つずつあります。有効な NIC が同じ種類のアドレスを複数持つことはできません。

TS エージェントに関する問題のトラブルシューティング

Firepower Management Center のテスト接続が失敗する

(ドメインユーザではなく) ローカルユーザとして TS エージェントサーバにログインしている場合、TS エージェントと Firepower Management Center とのテスト接続が失敗します。これは、デフォルトでは、TS エージェントがシステムプロセスにネットワーク上での通信を許可しないために発生します。

この問題を回避するには、次の手順を実行します。

- **TS エージェントの設定フィールド (16 ページ)** の説明に従って、[設定 (Configure)] タブページの [不明なトラフィック通信 (Unknown Traffic Communication)] をオンにしてトラフィックを許可します。
- ローカルユーザとしてではなく、ドメインユーザとして TS エージェントコンピュータにログインします。

TS エージェントがアップグレード時に再起動を要求する

マシンの IP アドレスが変更されない場合でも、アップグレード後に TS エージェントが IP アドレスの変更を報告し、サーバの再起動を要求することがあります。これは、TS エージェントが IP アドレスと次のレジストリキーの値の違いを検出するために発生します。

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

設定されたプライマリアダプタの IP アドレスとキー値が異なる場合、TS エージェントが変更を報告し、設定を保存してコンピュータを再起動するように指示されます。

これは、たとえば、コンピュータが再イメージ化またはバックアップから復元され、DHCP が新しい IP アドレスを割り当てた場合に発生することがあります。

エラーは無視できますが、いずれにしても、アップグレード後にコンピュータを再起動する必要があります。

Citrix Provisioning クライアントが起動に失敗する

Citrix Provisioning Server 用に設定した UDP ポートが無視するように TS エージェントを設定する必要があります。

TS エージェントの [予約ポート (Reserve Port(s))] フィールドで指定する値は、Citrix Provisioning の [最初と最後の UDP ポート番号 (First and Last UDP port numbers)] のポートのいずれかと一致する必要があります。



注意 正しいポートを指定しないと、クライアントの起動に失敗します。

TS エージェントの IP アドレスを保存する際の例外

まれに、無効な IP アドレスを使用して TS エージェント設定を保存しようとする、例外が表示されます。無効な IP アドレスは、次のいずれかになります。

- ネットワーク上の別のデバイスと同じ IP アドレス。
- TS エージェントアプリケーションが開いているときに、Windows で変更した静的 IP アドレス。

例外は次のとおりです。

- `System.ArgumentException` : 同じキーを持つ項目がすでに追加されています。(An item with the same key has already been added.)
- `System.NullReferenceException` : オブジェクト参照がオブジェクトのインスタンスに設定されていません。(Object reference not set to an instance of an object.)

回避策 : TS エージェントサーバの IP アドレスを有効な IP アドレスに設定し、TS エージェントの設定を保存して、サーバを再起動します。

ユーザエージェントに関する問題のトラブルシューティング

TS エージェントとユーザエージェントの両方を使用する場合、ユーザエージェントから TS エージェントの IP アドレスを除外することによって、重大ではないエラーのログを回避できます。TS エージェントとユーザエージェントの両方によって同じユーザが検出されると、重大ではないエラーがログに書き込まれます。

これを防ぐには、TS エージェントの IP アドレスがユーザエージェントによってログに記録されないようにします。詳細については、[Firepower ユーザエージェント コンフィギュレーションガイド \[英語\]](#) を参照してください。

解決済みの問題

解決済みの問題

不具合 ID 番号	説明
CSCvp10012	TS エージェントがインストールされている場合、Windows Server が応答しなくなることがなくなりました。
CSCvn28482	TAC ダンプの実行時に TS エージェントが応答しなくなることがなくなりました。さらに、ドライバフィルタを含む XML ファイルがダンプに追加されました。

TS エージェントの履歴

機能	バージョン
<ul style="list-style-type: none">• Citrix Provisioningのサポートが追加されました。• TS エージェントの [予約ポート (Reserve Port(s))] フィールドで指定する値は、Citrix Provisioning の [最初と最後の UDP ポート番号 (First and Last UDP port numbers)] のポートのいずれかと一致する必要があります。 <p>注意 正しいポートを指定しないと、クライアントの起動に失敗します。</p>	1.3

機能	バージョン
<ul style="list-style-type: none"> • サーバ上の IP アドレスの変更を検出し、設定を保存して再起動するように求めます。TS エージェントの設定フィールド (16 ページ) を参照してください。 • 以前のバージョンをアンインストールせずに、このバージョンにアップグレードできます。TS エージェントのインストールまたはアップグレード (13 ページ) を参照してください。 • [除外ポート (Exclude Port(s))]設定フィールドの名前が[予約ポート (Reserve Port(s))]に変更されました。TS エージェントの設定フィールド (16 ページ) を参照してください。 • エフェメラルポートのサポート。TS エージェントの設定フィールド (16 ページ) を参照してください。 • [モニタ (Monitor)]タブページでは、特定のセッションで TCP または UDP ポートの 50% 以上が使用されている場合に警告が表示されます。TS エージェントに関する情報の表示 (33 ページ) を参照してください。 • Least Recently Used ベースで割り当てられたユーザセッションポートの範囲。シスコ ターミナル サービス (TS) エージェントについて (1 ページ) を参照してください。 • トラブルシューティング情報を XML ファイルにエクスポートできます。TS エージェントに関する情報の表示 (33 ページ) を参照してください。 • Firepower Management Center にユーザセッションを再ストリーミングできます。TS エージェントに関する情報の表示 (33 ページ) を参照してください。 • TS エージェントがアンインストールされると、すべてのユーザセッションを終了しようとします。TS エージェントのアンインストール (38 ページ) を参照してください。 	1.2

機能	バージョン
<ul style="list-style-type: none"> • 最大ユーザセッションのデフォルトの最大数が200から30に変更されました。 • ポート範囲が200以上から5000以上に変更されました。 <p>これらの変更については、すべてTS エージェントの設定フィールド (16 ページ) で説明されています。</p>	1.1
<p>TS エージェント</p> <p>導入された機能。TS エージェントを使用すると、管理者はポートマッピングを使用してユーザアクティビティを追跡できます。TS エージェントは、ターミナルサーバにインストールされると、一定のポート範囲を個別のユーザセッションに割り当て、その範囲内のポートをユーザセッションにおけるTCPおよびUDP接続に割り当てます。システムは、ネットワーク上のユーザによる個別のTCPおよびUDP接続を識別するために一意のポートを使用します。</p>	1.0



第 2 章

TS エージェントのインストールと設定

- [TS エージェントのインストールまたはアップグレード \(13 ページ\)](#)
- [TS エージェント設定インターフェイスの開始 \(14 ページ\)](#)
- [TS エージェントの設定 \(14 ページ\)](#)
- [REST VDI ロールの作成 \(31 ページ\)](#)

TS エージェントのインストールまたはアップグレード

始める前に

- [サーバおよびシステム環境要件 \(2 ページ\)](#) の説明に従って、TS エージェントがお使いの環境でサポートされていることを確認してください。
- [現在のユーザセッションの終了 \(37 ページ\)](#) の説明に従って、現在のすべてのユーザセッションを終了してください。

ステップ 1 管理者特権を持つユーザとしてサーバにログインします。

ステップ 2 サポートサイトから、TS エージェントパッケージをダウンロードします。TSAgent-1.3.0.exe

(注) サイトから更新プログラムを直接ダウンロードします。ファイルを電子メールで転送すると、破損することがあります。

ステップ 3 [TSAgent-1.3.0.exe] を右クリックし、[管理者として実行 (Run as Administrator)] を選択します。

ステップ 4 [インストール (Install)] をクリックして、TS エージェントをインストールまたはアップグレードするための指示に従います。

TS エージェントを使用する前に、コンピュータを再起動する必要があります。

次のタスク

- [TS エージェント サービス コンポーネントの状態の表示 \(37 ページ\)](#) の説明に従って、TS エージェントが実行されていることを確認します。

- [TS エージェント プロセスの開始と停止 \(38 ページ\)](#) の説明に従って、TS エージェントを起動します。
- [TS エージェントの設定 \(14 ページ\)](#) の説明に従って、TS エージェントを設定します。

以前のバージョンの TS エージェントからアップグレードし、Citrix Provisioning を使用している場合は、アップグレード後に [予約ポート (Reserve Port(s))] フィールドに 6910 と入力する必要があります。



(注) TS エージェント インストーラによって .NET Framework の失敗が報告された場合、Windows Update を実行し、TS エージェントのインストールを再試行してください。

TS エージェント設定インターフェイスの開始

cite

TS エージェントのショートカットがデスクトップ上にある場合は、ショートカットをダブルクリックします。そうでない場合、TS エージェント設定インターフェイスを起動するには、次の手順を使用します。

ステップ 1 管理者特権を持つユーザとしてサーバにログインします。

ステップ 2 C:\Program Files (x86)\Cisco\Terminal Services Agent を開きます。

ステップ 3 TS エージェントのプログラム ファイルを表示します。

(注) このプログラム ファイルは、表示専用です。これらのファイルは削除、移動、または変更しないでください。

ステップ 4 TSAgentApp ファイルをダブルクリックして、TS エージェントを開始します。

TS エージェントの設定

TS エージェントを設定するには、TS エージェントインターフェイスを使用します。変更を有効にするには、変更を保存してサーバを再起動する必要があります。

始める前に

- Firepower システムに接続する場合は、『*Firepower Management Center Configuration Guide*』の説明に従って、お使いのサーバがモニタするユーザをターゲットにした Active Directory レルムを 1 つ以上設定し、有効化します。
- Firepower システムに接続する場合は、REST VDI 特権を持つユーザ アカウントを設定します。

REST VDI ロールの作成 (31 ページ) の説明に従って、Firepower Management Center 内に REST VDI ロールを作成する必要があります。

- Firepower システムにすでに接続しており、かつ別の Firepower Management Center に接続するように TS エージェントの設定を更新する場合は、新しい設定を保存する前に、現在のすべてのユーザセッションを終了する必要があります。詳細については、[現在のユーザセッションの終了 \(37 ページ\)](#) を参照してください。
- TS エージェント サーバと Firepower システムの時計を同期させます。
- [TS エージェントの設定フィールド \(16 ページ\)](#) の説明に従って、設定フィールドを確認し、理解してください。

-
- ステップ 1** [TS エージェント設定インターフェイスの開始 \(14 ページ\)](#) の説明に従って、TS エージェントをインストールしたサーバで、TS エージェントを開始します。
- ステップ 2** [構成 (Configure)] をクリックします。
- ステップ 3** タブ ページの [全般設定 (General Settings)] セクションに移動します。
- ステップ 4** [最大ユーザセッション (Max User Sessions)] の値を入力します。
- ステップ 5** ポート変換および通信に使用する [サーバ NIC (Server NIC)] を選択します。
- サーバの IP アドレスが後で変更された場合は、設定を保存し、変更を有効にするためにサーバを再起動するように求められます。
- ステップ 6** [システム ポート (System Ports)] および [ユーザ ポート (User Ports)] の値を入力します。有効な設定では、システム ポートとユーザ ポートの範囲が重複しません。
- ステップ 7** [予約ポート (Reserve Port(s))] の値をコンマ区切りのリストとして入力します。
- [予約ポート (Reserve Port(s))] には、Citrix MA クライアントのポート (2598) 、Citrix Provisioning のポート (6910) 、Windows ターミナルサーバのポート (3389) に想定される値が自動的に設定されます。Citrix MA クライアントと Windows ターミナルサーバのポートは、除外する必要があります。
- Citrix Provisioning を使用していて、以前の TS エージェントバージョンからアップグレードする場合は、このフィールドに 6910 と入力する必要があります。
- ステップ 8** タブの [Firepower Management Center REST API 接続 (Firepower Management Center REST API Connection)] 設定セクションに移動します。
- ステップ 9** [ホスト (Host)]、[ホスト名/IP アドレス (Hostname/IP Address)]、および [ポート (Port)] の値を入力します。
- Firepower Management Center には、[ポート (Port)] 443 が必要です。ISE/ISE-PIC には、[ポート (Port)] 9094 が必要です。
- ステップ 10** [ユーザ名 (Username)] と [パスワード (Password)] を入力します。
- ステップ 11** 必要に応じ、2 番目の行のフィールドで手順 9 と 10 を繰り返す、スタンバイ (フェールオーバー) 接続を設定します。
- ステップ 12** [テスト (Test)] をクリックして、TS エージェントとシステムの間 REST API 接続をテストします。

プライマリとセカンダリの Firepower Management Center を設定している場合は、セカンダリへのテスト接続が失敗します。これは想定されている動作です。TS エージェントは、アクティブな Firepower Management Center と常に通信します。プライマリがダウンして非アクティブの Firepower Management Center になった場合、TS エージェントは、セカンダリの（アクティブになった） Firepower Management Center と通信します。

ステップ 13 [保存 (Save)] をクリックして、デバイスのリポートを確認します。

TS エージェントの設定フィールド

TS エージェントの設定には、次のフィールドを使用します。

全般設定

表 1: 全般設定フィールド

フィールド	説明	例
[予約ポート (Reserve Port(s))]		通常、次のいずれかです。 <ul style="list-style-type: none">• 2598、3389 (Citrix MA クライアントおよび Windows ターミナル サーバのポート)• 2598、3389、6910 (Citrix MA クライアント、Windows ターミナルサーバ、および Citrix Provisioning のポート)

フィールド	説明	例
	<p>TS エージェントに無視させるポート。除外したいポートをコンマ区切りのリストとして入力します。</p> <p>[予約ポート (Reserve Port(s))]には、Citrix MA クライアントのポート (2598)、Citrix Provisioning のポート (6910)、Windows ターミナルサーバのポート (3389) のデフォルト値が TS エージェントによって自動的に設定されます。正しいポートを除外しないと、これらのポートを必要とするアプリケーションが失敗する可能性があります。</p> <p>TS エージェントの [予約ポート (Reserve Port(s))] フィールドで指定する値は、Citrix Provisioning の [最初と最後の UDP ポート番号 (First and Last UDP port numbers)] のポートのいずれかと一致する必要があります。</p> <p>注意 正しいポートを指定しないと、クライアントの起動に失敗します。</p> <p>(注) お使いのサーバ上のプロセスが [システムポート (System Ports)] の範囲にならないポートを使用またはリスンしている場合、そのポートは、[予約ポート (Reserve Port(s))] フィールドを使用して手動で除外する必要があります。</p>	

フィールド	説明	例
	<p>(注) サーバにクライアントアプリケーションがインストールされていて、そのアプリケーションが特定のポート番号を使用するソケットにバインドするよう設定されている場合、[予約ポート (Reserve Port(s))]フィールドを使用して、そのポートを変換から除外する必要があります。</p>	
最大ユーザセッション (Max User Sessions)	<p>TS エージェントにモニタさせるユーザセッションの最大数。単一のユーザが一度に複数のユーザセッションを実行する場合があります。</p> <p>このバージョンのTS エージェントは、デフォルトで29のユーザセッションをサポートし、最大199のユーザセッションをサポートします。</p>	29 (このバージョンのTS エージェントがサポートする最大値)

フィールド	説明	例
サーバ NIC (Server NIC)		Ethernet 2 (192.0.2.1) (サーバ上の NIC)

フィールド	説明	例
	<p>このバージョンの TS エージェントでは、ポート変換およびサーバシステム間の通信に、単一のネットワーク インターフェイス コントローラ (NIC) を使用することができます。サーバに有効な NIC が 2 つ以上存在する場合、TS エージェントは、設定の際に指定されたアドレスに対してのみポートの変換を実行します。</p> <p>TS エージェントは、このフィールドに、TS エージェントがインストールされているサーバの各 NIC の IPv4 アドレスおよび/または IPv6 アドレスを自動的に設定します。有効な NIC には必ず、IPv4 もしくは IPv6 のアドレスが 1 つだけ、または各タイプのアドレスが 1 つずつあります。有効な NIC が同じ種類のアドレスを複数持つことはできません。</p> <p>(注) サーバの IP アドレスが変更された場合は、設定を保存し、変更を有効にするためにサーバを再起動するように求められます。</p> <p>(注) サーバに接続されているデバイスで、ルータアドバタイズメントメッセージを無効にする必要があります。ルータアドバタイズメントが有効になっていると、デバイスがサーバ上の NIC に複数の IPv6</p>	

フィールド	説明	例
	アドレスを割り当て、TSエージェントで使用するNICを無効にしてしまう可能性があります。	

フィールド	説明	例
システム ポート (System Ports)		[開始 (Start)] を 10000 に設定し、[範囲 (Range)] を 5000 に設定

フィールド	説明	例
	<p>システム プロセスに使用するポートの範囲。TS エージェントは、このアクティビティを無視します。[開始 (Start)] ポートを設定し、範囲を開始する場所を指定します。[範囲 (Range)] の値を設定し、個々のシステム プロセスに割り当てるポートの数を指定します。</p> <p>シスコが推奨する [範囲 (Range)] の値は、5000 以上です。TS エージェントでシステム プロセス用のポートが頻繁に不足する場合は、[範囲 (Range)] の値を大きくします。</p> <p>(注) システムプロセスが指定された [システムポート (System Ports)] の範囲外のポートを要求する場合は、そのポートを [除外ポート (Exclude Port(s))] フィールドに追加します。システムプロセスによって使用されるポートを [システムポート (System Ports)] の範囲に指定するか除外するかしないと、システムプロセスが失敗する可能性があります。</p> <p>TS エージェントは、次の数式を使用して、[終了 (End)] の値を自動的に設定します。</p> $([Start\ value] + [Range\ value]) - 1$ <p>入力の結果、[終了 (End)] の</p>	

フィールド	説明	例
	値が [ユーザ ポート (User Ports)] の [開始 (Start)] の値を超える場合、[開始 (Start)] および [範囲 (Range)] の値を調整する必要があります。	

フィールド	説明	例
ユーザ ポート (User Ports)	<p>ユーザ用に指定するポートの範囲。[開始 (Start)]ポートを設定し、範囲を開始する場所を指定します。[範囲 (Range)]の値を設定し、個々のユーザセッションにおける TCP または UDP 接続に割り当てるポートの数を指定します。</p> <p>(注) ICMP トラフィックは、ポートがマッピングされずに渡されます。</p> <p>シスコが推奨する [範囲 (Range)]の値は、1000 以上です。TS エージェントでユーザ トラフィック用のポートが頻繁に不足する場合は、[範囲 (Range)]の値を大きくします。</p> <p>(注) 使用されているポートの数が [範囲 (Range)]の値を超えると、ユーザ トラフィックがブロックされます。</p> <p>TS エージェントは、次の数式を使用して、[終了 (End)]の値を自動的に設定します。</p> $[\text{Start value}] + ([\text{Range value}] * [\text{Max User Sessions value}]) - 1$ <p>入力の結果、[終了 (End)]の値が 65535 を超える場合、[開始 (Start)]および [範囲 (Range)]の値を調整する必要があります。</p>	<p>[開始 (Start)]を 15000 に設定し、[範囲 (Range)]を 1000 に設定</p>

フィールド	説明	例
エフェメラル ポート	TS エージェントがモニタできるように、エフェメラルポートの範囲（ダイナミックポートとも呼ばれる）を入力します。	[開始 (Start)] を 49152 に設定し、[範囲 (Range)] を 16384 に設定

フィールド	説明	例
不明なトラフィック通信		適用対象外

フィールド	説明	例
	<p>[許可 (Permit)] をオンにして、TS エージェントがシステムポート経由のトラフィックを許可できるようにします。ただし、TS エージェントはポートの使用状況を追跡しません。システムポートは、ローカルシステムアカウントまたは他のローカルユーザアカウントによって使用されます (ローカルユーザアカウントはTS エージェントサーバにのみ存在します。対応する Active Directory アカウントはありません)。このオプションを選択すると、次のタイプのトラフィックを許可できます。</p> <ul style="list-style-type: none"> • ブロックされるのではなく、ローカルシステムアカウント (サーバメッセージブロック (SMB) など) によって実行されるトラフィックを許可します。ユーザが Active Directory に存在しないため、Firepower Management Center はこのトラフィックを不明なユーザからのトラフィックとして識別します。 <p>このオプションを有効にすると、ローカルシステムアカウントを使用してTS エージェントサーバにログインしている場合、Firepower Management Center との接続を正常にテストできます。</p> <ul style="list-style-type: none"> • ユーザまたはシステムセッションがその範囲内の使用可能なすべての 	

フィールド	説明	例
	<p>ポートを使い果たすと、TS エージェントはエフェメラルポート経由のトラフィックを許可します。このオプションは、トラフィックを有効にしません。 Firepower Management Center は、不明なユーザからのトラフィックとして識別します。</p> <p>これは、ドメインコントローラの更新、認証、Windows Management Interface (WMI) クエリなど、システムの健全性を維持するためにシステムポートが必要な場合に特に役立ちます。</p> <p>システムポートのトラフィックをブロックするには、オフにします。</p>	

REST API 接続の設定

プライマリのシステムアプライアンスに加え、必要に応じてスタンバイ（フェールオーバー）のシステムアプライアンスの接続を設定することができます。

- システムアプライアンスがスタンドアロンの場合、REST API 接続フィールドの2番目の行は空白のままにします。
- システムアプライアンスをスタンバイ（フェールオーバー）アプライアンスとともに展開している場合、1番目の行はプライマリアプライアンスへの接続の設定に、2番目の行はスタンバイ（フェールオーバー）アプライアンスへの接続の設定に使用します。

表 2: REST API 接続設定用のフィールド

フィールド	説明	例
ホスト名/IP アドレス (Hostname/IP Address)	システムアプライアンスのホスト名または IP アドレス。	192.0.2.1

フィールド	説明	例
ポート (Port)	システムが REST API 通信に使用するポート。(Firepower Management Center では、通常はポート 443 が使用されます)。	443
ユーザ名とパスワード	接続のためのクレデンシャル。 • Firepower システムでは、Firepower Management Center で REST VDI 特権を持つユーザのユーザ名とパスワードが必要です。このユーザの設定に関する詳細については、『 <i>Firepower Management Center Configuration Guide</i> 』を参照してください。	n/a

REST VDI ロールの作成

TS エージェントを Firepower Management Center に接続するには、お使いの Firepower ユーザが REST VDI ロールを持っている必要があります。REST VDI は、デフォルトでは定義されていません。ロールを作成し、TS エージェントの設定に使用するユーザに割り当てる必要があります。

ユーザおよびロールの詳細については、『*Firepower Management Center Configuration Guide*』を参照してください。

-
- ステップ 1** Firepower Management Center にロール作成の権限を持つユーザとしてログインします。
- ステップ 2** [システム (System)] > [ユーザ (Users)] をクリックします。
- ステップ 3** [ユーザロール (User Roles)] タブをクリックします。
- ステップ 4** [ユーザロール (User Roles)] タブ ページで、[ユーザロールの作成 (Create User Role)] をクリックします。
- ステップ 5** [名前 (Name)] フィールドに、REST VDI と入力します。
ロール名では、大文字と小文字が区別されません。
- ステップ 6** [メニューベースのアクセス許可 (Menu-Based Permissions)] セクションで、[REST VDI] をオンにし、[REST VDI の変更 (Modify REST VDI)] もオンになっていることを確認します。

ステップ 7 [保存 (Save)] をクリックします。

ステップ 8 ロールを TS エージェントの設定に使用するユーザに割り当てます。



第 3 章

TS エージェントデータの表示

- [TS エージェントに関する情報の表示 \(33 ページ\)](#)
- [接続ステータスの表示 \(35 ページ\)](#)
- [TS エージェントユーザ、ユーザセッション、および TCP/UDP 接続データの Firepower Management Center での表示 \(35 ページ\)](#)

TS エージェントに関する情報の表示

ネットワークにおける現在のユーザセッションと、各セッションに割り当てられているポートの範囲を表示するには、次の手順を使用します。このデータは読み取り専用です。





ステップ 1 [TS エージェント設定インターフェイスの開始 \(14 ページ\)](#) の説明に従って、TS エージェントをインストールしたサーバで、TS エージェント インターフェイスを開始します。

ステップ 2 [モニタ (Monitor)] タブをクリックします。次のカラムが表示されます。

- [REST サーバ ID (REST Server ID)] : 情報を報告している Firepower Management Center または ISE/ISE-PIC サーバのホスト名または IP アドレス。ハイ アベイラビリティ設定を適用している場合、この情報が役に立ちます。
- [送信元 IP (Source IP)] : IPv4 および/または IPv6 形式でユーザの IP アドレスの値を表示します。IPv4 と IPv6 の両方のアドレスが設定されており、新しいセッションが作成されたばかりのときは、IPv4 と IPv6 の両方のアドレスが別々の行に表示されます。
- [状態 (Status)] : ユーザへのポートの割り当ての状態が表示されます。詳細については、[接続ステータスの表示 \(35 ページ\)](#) を参照してください。
- [セッション ID (Session ID)] : ユーザのセッションを識別する番号。ユーザは、一度に複数のセッションを持つことができます。
- [ユーザ名 (Username)] : セッションに関連付けられているユーザ名。
- [ドメイン (Domain)] : ユーザがログインした Active Directory ドメインの名前。
- [ポート範囲 (Port Range)] : ユーザに割り当てられているポート範囲。(値 0 は、ポートの割り当てに問題があることを示します。詳細については、[接続ステータスの表示 \(35 ページ\)](#) を参照してください)。

- [TCP ポート使用率 (TCP Ports Usage)] および [UDP ポート使用率 (UDP Ports Usage)] : ユーザごとに割り当てられたポートの割合が表示されます。割合が 50% を超えると、フィールドの背景が黄色になります。割合が 80% を超えると、フィールドの背景が赤色になります。
- [ログイン日付 (Login Date)] : ユーザがログインした日付。

ステップ 3 次の表に、実行可能なアクションを示します。

項目	説明
列見出しをクリック	テーブル内のデータをその列でソートします。
	[ユーザ名でフィルタ (Filter by Username)] 検索フィールドに、ユーザ名の一部または全体を入力します。
	クリックすると、このタブページに表示されるセッションが更新されます。
	TS エージェントに関する次のトラブルシューティング情報をテキストファイルとしてエクスポートします。 <ul style="list-style-type: none"> • TS エージェント設定データを含む XML ファイル • <code>netstat -a -n -o</code> コマンドからの出力 • Windows タスクリスト • 実行中のドライバのリスト
	1 つ以上のセッションの横にあるボックスをオンにして、それらのセッションを Firepower Management Center に再ストリーミングします。これは、Firepower Management Center でユーザサービスが失敗した場合に使用できます。 たとえば、ユーザサービスが Firepower Management Center で失敗した後に、ユーザが TS エージェントサーバにログインするとします。このオプションを使用すると、ユーザサービスの復元後にユーザセッションを再送信できます。これにより、そのユーザの [ステータス (Status)] 列に [成功 (Success)] が表示されます。

接続ステータスの表示

TS エージェントがインストールされているターミナル サービスにユーザがログインすると、新しいシステムセッションが作成され、このセッションにポートの範囲が割り当てられます。その結果は Firepower Management Center または ISE に送信され、管理対象デバイスに配布されます。

T[モニタ (Monitor)] タブ ページでは、ポートの範囲が Firepower Management Center または ISE に正常に送信されたかを確認することができます。プロセスが失敗する理由には、次などがあります。

- ネットワークの接続性に関する問題
 - 無効な VDI クレデンシヤル
- トークンの期限切れ
- レルムに設定されたドメイン名が不正

ステップ 1 [TS エージェント設定インターフェイスの開始 \(14 ページ\)](#) の説明に従って、TS エージェントをインストールしたサーバで、TS エージェント インターフェイスを開始します。

ステップ 2 [モニタ (Monitor)] タブをクリックします。

ステップ 3 [状態 (Status)] カラムには、次のいずれかの値が表示されます。

- [保留中 (Pending)] : アクションは保留中で、まだ完了していません。
- [失敗 (Failed)] : アクションは失敗しました。[失敗 (Failed)] という単語をクリックすると、エラーメッセージが表示されます。エラーが Firepower Management Center との通信障害を示している場合は、[TS エージェントに関する情報の表示 \(33 ページ\)](#) の説明に従い、そのセッションのトラフィックを再ストリームしてみます。
- [成功 (Success)] : アクションは正常に完了しました。

TS エージェントユーザ、ユーザセッション、および TCP/UDP 接続データの Firepower Management Center での表示

TS エージェントによって報告されたデータを表示するには、次の手順を使用します。Firepower Management Center の各種テーブルの詳細については、『*Firepower Management Center Configuration Guide*』を参照してください。

-
- ステップ 1** お使いのサーバがモニタするユーザをターゲットにしたレلمを設定した Firepower Management Center にログインします。
- ステップ 2** [ユーザ (Users)] テーブルにユーザを表示するには、[分析 (Analysis)]>[ユーザ (Users)]>[ユーザ (Users)]の順に選択します。TS エージェントのユーザセッションが現在アクティブである場合、Firepower Management Center は、[現在の IP (Current IP)]、[終了ポート (End Port)]、および[開始ポート (Start Port)]の各カラムに値を投入します。
- ステップ 3** [ユーザアクティビティ (User Activity)] テーブルにユーザセッションを表示するには、[分析 (Analysis)]>[ユーザ (Users)]>[ユーザアクティビティ (User Activity)]の順に選択します。TS エージェントからユーザセッションが報告された場合、Firepower Management Center は、[現在の IP (Current IP)]、[終了ポート (End Port)]、および[開始ポート (Start Port)]の各カラムに値を投入します。
- ステップ 4** [接続イベント (Connection Events)] テーブルに TCP/UDP 接続を表示するには、[分析 (Analysis)]>[接続 (Connections)]>[イベント (Events)]の順に選択します。Firepower Management Center は、[イニシエータ/レスポンド IP (Initiator/Responder IP)] フィールドに接続を報告した TS エージェントの IP アドレスを、[送信元ポート/ICMP タイプ (Source Port/ICMP Type)] フィールドに TS エージェントが接続に割り当てたポートを、それぞれ入力します。
-



第 4 章

TS エージェントの管理

- [現在のユーザセッションの終了](#) (37 ページ)
- [TS エージェント サービス コンポーネントの状態の表示](#) (37 ページ)
- [TS エージェント プロセスの開始と停止](#) (38 ページ)
- [TS エージェント アクティビティ ログのサーバでの表示](#) (38 ページ)
- [TS エージェントのアンインストール](#) (38 ページ)

現在のユーザセッションの終了

ネットワークからユーザをログオフしてそのセッションを終了するには、次の手順を使用します。

-
- ステップ 1** 管理者特権を持つユーザとして TS エージェント サーバにログインします。
 - ステップ 2** [開始 (Start)]>>[すべてのプログラム (All Programs)]>[タスク マネージャ (Task Manager)]を開きます。
 - ステップ 3** [詳細の表示 (More Details)]をクリックして、ウィンドウを展開します。
 - ステップ 4** [ユーザ (Users)]タブをクリックします。
 - ステップ 5** (任意) セッション終了の対象ユーザに通知を行う場合、当該のユーザセッションを右クリックし、[メッセージの送信 (Send message)]を選択します。
 - ステップ 6** 当該のユーザセッションを右クリックし、[サインオフ (Sign off)]を選択します。
 - ステップ 7** [ユーザのサインアウト (Sign out user)]をクリックし、アクションを確定します。
-

TS エージェント サービス コンポーネントの状態の表示

TS エージェント サービス コンポーネントが実行されていることを確認するには、次の手順を使用します。サービス コンポーネントの詳細については、[シスコターミナルサービス \(TS\) エージェントについて](#) (1 ページ) を参照してください。

-
- ステップ1 管理者特権を持つユーザとしてサーバにログインします。
 - ステップ2 [開始 (Start)]>[ツール (Tools)]>[サービス (Services)]を開きます。
 - ステップ3 CiscoTSAgent に移動し、[状態 (Status)]を表示します。
 - ステップ4 (任意) TS エージェント サービス コンポーネントが停止している場合は、[TS エージェント プロセスの開始と停止 \(38 ページ\)](#) の説明に従って、TS エージェント サービスを開始してください。
-

TS エージェント プロセスの開始と停止

TS エージェント サービス コンポーネントを開始または停止するには、次の手順を使用します。

-
- ステップ1 管理者特権を持つユーザとしてサーバにログインします。
 - ステップ2 [開始 (Start)]>[管理ツール (Administrative Tools)]>[サービス (Services)]を開きます。
 - ステップ3 CiscoTSAgent に移動し、右クリックして、コンテキストメニューを表示します。
 - ステップ4 [開始 (Start)]または[停止 (Stop)]を選択し、TS エージェント サービスを開始または停止します。
-

TS エージェント アクティビティ ログのサーバでの表示

サポートから求められた場合、次の手順に従って、サービスコンポーネントのアクティビティログを表示します。

[ツール (Tools)]>[イベントビューア (Event Viewer)]>[アプリケーションおよびサービスのログ (Applications and Services Log)]>[ターミナル サービス エージェント ログ (Terminal Services Agent Log)]を開きます。

TS エージェントのアンインストール

サーバから TS エージェントをアンインストールするには、次の手順を使用します。TS エージェントをアンインストールすると、インターフェイス、サービス、およびドライバがサーバから削除されます。TS エージェントをアンインストールすると、Firepower Management Center に報告されたアクティブなユーザセッションも終了します。強力な暗号化への変更は、削除されません。

-
- ステップ1 管理者特権を持つユーザとしてサーバにログインします。
 - ステップ2 [開始 (Start)]>[コントロールパネル (Control Panel)]を開きます。

ステップ 3 [すべてのコントロールパネル項目 (All Control Panel Items)] > [プログラムと機能 (Programs and Features)] をクリックします。

ステップ 4 [ターミナル サービス エージェント (Terminal Services Agent)] を右クリックし、[アンインストール (Uninstall)] を選択します。
